UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
FACULDADE DE ARTES, ARQUITETURA E COMUNICAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO MESTRADO EM MÍDIA E TECNOLOGIA

PROTEÇÃO DE DADOS E O ESTUDO DA LGPD

DANIELE VINCENZI VILLARES BURKART

BAURU

2021

DANIELE VINCENZI VILLARES BURKART

PROTEÇÃO DE DADOS E O ESTUDO DA LGPD

Dissertação de Mestrado, apresentado ao Programa de Pós-graduação em Mídia e Tecnologia, da Faculdade de Artes, Arquitetura e Comunicação da Universidade Estadual Paulista Júlio de Mesquita Filho, para obtenção do título de Mestre em Mídia e Tecnologia, sob a orientação do Prof. Dr. Francisco Machado Filho.

BAURU

2021

Burkart, Daniele Vincenzi Villares.
Proteção de dados e o estudo da LGPD / Daniele Vincenzi Villares Burkart, 2021
141 f. : il.

Orientador: Francisco Machado Filho

Dissertação (Mestrado)–Universidade Estadual Paulista. Faculdade de Arquitetura, Artes e Comunicação, Bauru, 2021

1. Direitos individuais. 2. Privacidade. 3. Lei geral de proteção de dados. 4. Cultura organizacional. 5. Tratamento de dados pessoais. I. Universidade Estadual Paulista. Faculdade de Arquitetura, Artes e Comunicação. II. Título.

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Bauru

ATA DA DEFESA PÚBLICA DA DISSERTAÇÃO DE MESTRADO DE DANIELE VINCENZI VILLARES BURKART, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM MÍDIA E TECNOLOGIA, DA FACULDADE DE ARQUITETURA, ARTES E COMUNICAÇÃO - CÂMPUS DE BAURU.

Aos 03 dias do mês de março do ano de 2021, às 09:00 horas, por meio de Videoconferência, realizou-se a defesa de DISSERTAÇÃO DE MESTRADO de DANIELE VINCENZI VILLARES BURKART, intitulada **Proteção de dados e o estudo da LGPD**. A Comissão Examinadora foi constituida pelos seguintes membros: Professor Assistente Doutor FRANCISCO MACHADO FILHO (Orientador(a) - Participação Virtual) do(a) Departamento de Comunicação Social da Faculdade de Arquitetura, Artes e Comunicação / Universidade Estadual Paulista , Professor Doutor ALCIDES EDUARDO DOS REIS PERON (Participação Virtual) do(a) Departamento de Sociologia / Universidade de São Paulo, Professora Associada VÂNIA CRISTINA PIRES NOGUEIRA VALENTE (Participação Virtual) do(a) Departamento de Artes e Representação Gráfica da Faculdade de Arquitetura, Artes e Comunicação / Universidade Estadual Paulista . Após a exposição pela mestranda e arguição pelos membros da Comissão Examinadora que participaram do ato, de forma presencial e/ou virtual, a discente recebeu o conceito final:_ _ APROVADA _ _ . Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelo(a) Presidente(a) da Comissão Examinadora.

Professor Assistente Doutor FRANCISCO MACHADO FILHO

DANIELE VINCENZI VILLARES BURKART

PROTEÇÃO DE DADOS E O ESTUDO DA LGPD

Área de Concentração: Ambientes Midiáticos e Tecnológicos

Linha de Pesquisa: Gestão Midiática e Tecnológica

Banca Examinadora:

Presidente/Orientador: Instituição: Prof. Dr. Francisco Machado Filho

Prof. 1 Unesp Bauru: Prof. Dr. Vânia Cristina Pires Nogueira Valente

Prof. 2 USP: Prof. Prof. Dr. Alcides Perón

Resultado: Aprovado

Bauru, 03 de março de 2021

Dedico este trabalho primeiramente a Deus, por me permitir estar aqui, aprendendo e evoluindo. À minha família pelo apoio durante esse tempo e em especial ao meu filho e marido por compreenderem a necessidade de minha dedicação ao mestrado que foi realizado com muito amor.

AGRADECIMENTOS

À Deus, por me dar força e saúde para seguir este sonho e alcançar o resultado esperado.

À minha família, por toda a compreensão e apoio que foram fundamentais na busca do conhecimento e na realização deste sonho.

A todos os professores do programa, que contribuíram com meu aperfeiçoamento e aprendizagem, durante esses quase 3 anos de estudos e dedicação.

À equipe da UNESP – FAAC – Bauru por facilitar todo o processo necessário para a execução do meu mestrado.

Ao meu orientado Prof. Dr. Francisco Machado Filho pela paciência, comprometimento e confiança depositada em mim durante todo o trabalho.

A todos que fizeram parte da minha formação direta ou indiretamente.

“A tua ansiedade ou o teu receio não alterarão o curso das horas. Aguarde o que há de suceder, sem que te imponhas sofrimento desde a véspera.”

Joanna de Ângelis

BURKART, D. V. V. PROTEÇÃO DE DADOS E O ESTUDO DA LGPD, 2021, 96 f. Trabalho de Conclusão de Mestrado Mídia e Tecnologia – FAAC – UNESP, sob orientação da Prof. Dr. Francisco Machado Filho, Bauru, 2021.

RESUMO

Este trabalho tem como objetivo estudar a nova Lei geral de proteção de dados (LGPD), lei Nº 13.709, de 14 de agosto de 2018 e refletir sobre as lacunas existentes entre os direitos individuais e a garantia da privacidade como consequência da nova Lei geral de proteção de dados, que entrou em vigor em setembro de 2020 e trouxe um grande impacto na sociedade, que precisa se adaptar os princípios e bases legais descritos na lei, além de se tornar facilitador dos direitos adquiridos pelos titulares de dados. Por meio de estudo da legislação atual e com o embasamento teórico necessário para compreender os impactos causados na sociedade, procedeu-se à observação da abrangência da LGPD no território brasileiro, e à identificação das lacunas existentes entre os direitos individuais e a garantia da privacidade como consequência da nova Lei geral de proteção de dados, criando a necessidade de uma educação tecnológica em uma era de informatização das informações.

Palavras-chave: direitos individuais; privacidade; Lei geral de proteção de dados; cultura organizacional; tratamento de dados pessoais.

BURKART, D. V. V. DATA PROTECTION AND THE STUDY OF LGPD, 2021, 96 p. Paperwork of Conclusion of Media and Technology Master Degree – FAAC – UNESP, under orientation of Prof. Dr. Francisco Machado Filho, Bauru, 2021.

ABSTRACT

The aim of this paperwork is to study the new General Data Protection Regulation (LGPD), law No. 13.709, August 14, 2018 and reflect upon the existing gaps between the individual rights and the privacy guarantee as a consequence of the new General Data Protection Regulation, which was put into effect in September 2020 and brought a great impact in the society that needs to adapt to the principles and to the legal bases described in the law, apart from becoming a facilitator of the rights acquired by the data holders. By studying the current legislation and with the necessary theoretical background to understand the impacts caused in the society, the observation of the comprehensiveness of the LGPD in the Brazilian territory was carried out, as well as the identification of the existing gaps between the individual rights and the privacy guarantee as a consequence of this new General Data Protection Regulation, creating the necessity of a technological education in an era of computerization of information.

Key words: individual rights; privacy; General Data Protection Regulation; organizational culture; treatment of personal data.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO 1: CARACTERIZAÇÃO DA PESQUISA

1.1 Introdução

Com a inserção da tecnologia cada vez mais predominante na vida das pessoas, os dados pessoais dos indivíduos na sociedade estão mais vulneráveis, pois a informação tornou-se relevante para o curso do mercado, determinando tendências e necessidades, marcando assim a nova era da informatização[1]. Esta nova era, se alimenta de dados que são tratados e separados em padrões específicos e conhecidos, transformando-os assim, em informações que geram o conhecimento por meio da inteligência aplicada. Dessa forma, a utilização em massa das informações pelas organizações com fins lucrativos, tornou-as vulneráveis às violações de dados pessoais, que estão cada vez mais constantes na sociedade brasileira. Com o objetivo principal descrito na lei de proteger os dados pessoais e garantir um tratamento dos dados de forma correta pelas organizações, a nova Lei geral de proteção de dados – LGPD, lei Nº 13.709, entrou em vigor em setembro de 2020, na tentativa de minimizar o acesso das informações por pessoas ou organizações sem uma prévia autorização e conhecimento do titular dos dados. Apesar da tentativa em proteger os dados pessoais, observa-se o direito individual da pessoa, a qual permite o acesso de seus dados pessoais pelas organizações, sem o entendimento real do objetivo dessa disponibilização dos dados e de suas consequências para a sociedade como um todo.

Apesar do conhecimento de cada indivíduo sobre o valor de seus dados, barganhas[2] acontecem constantemente, obrigando os indivíduos a disponibilizar informações pessoais para finalidades gerais, como na aquisição de produtos e serviços. Essas informações, disponibilizadas a partir do consentimento, podem ser tratadas conforme finalidades descritas e pré-aprovadas pelo titular de dados. Dessa forma, esse tratamento não está sujeito à penalização da nova Lei geral de proteção de dados, a qual parte do princípio que os dados poderão ser tratados quando houver a permissão do titular de dados para os fins estabelecidos em termos de adesão aceitos ou em casos onde existe um motivo legal para o tratamento desses dados.

O trabalho foi organizado em seis capítulos. O capítulo 1 apresenta a introdução deste trabalho juntamente com a justificativa de sua necessidade e os objetivos gerais e específicos. No capítulo 2, é abordado os conceitos de dados e informação, bem como o

[1] **A Nova era da informatização** consiste em momento no qual os principais grupos sociais exercem funções as quais, serão aqueles formados pelos trabalhadores da área do conhecimento. Fonte: Rocha (2005).
[2] **As barganhas** acontecem constantemente, baseando-se na personalização e serviços de filtragens, em troca de grandes quantidades de dados pessoais, disponibilizados pela própria pessoa. (PARISER, 2012, p. 20).

processo de transformação dos dados em conhecimento, mostrando a geração de valor dos dados pessoais e a definição de proteção de dados pessoais, motivadores principais para a criação da nova legislação. Além disso, neste capítulo, contém explicações sobre o processo de violação de dados pessoais e a minimização das vulnerabilidades. No capítulo 3, é exposta a estrutura da Lei geral de proteção de dados, as novas obrigações em que a empresa está sujeita, os novos direitos dos titulares de dados, as bases legais previstas em lei e seus princípios. Para finalizar este capítulo, são apontadas informações a respeito de como uma empresa deve proceder no caso de violação de dados pessoais e como os indivíduos podem agir caso seus dados sejam violados e caso haja prejuízos com a eventual violação. O capítulo 4 discorre a respeito dos impactos da LGPD e de sua abrangência dentro do território brasileiro, além de apresentar medidas e técnicas utilizadas para a aderência à nova lei, bem como o que acontece em outros países que já possuem uma lei de proteção de dados em vigor. No capítulo 5, são comentadas as entrevistas realizadas com dois especialistas no assunto com a finalidade de suscitar discussões ainda existentes na interpretação da lei para minimizar as contradições encontradas. Para conclusão do trabalho, no capítulo 6, encontram-se as considerações finais, apontadas conforme estudo realizado.

1.2 Justificativa

A presente pesquisa parte incialmente da percepção empírica em que os dados pessoais atingiram valores superiores aos produtos tangíveis, como o petróleo, conforme Ferreira (2019). O processo de transformação dos dados em informação, para utilização na criação de estratégias assertivas, visa à lucratividade, além de posição política, social e econômica no Brasil.

A escolha desse tema foi motivada pela criação da nova Lei geral de proteção de dados (LGPD) e pelas consequências causadas anteriormente quando não existia uma regulamentação nesse sentido. Conforme sugeriu uma pesquisa publicada pelo Tecmundo (2020) e realizada pelo Instituto Ponemon, 63% das pequenas e médias empresas sofreram incidentes com vazamento de dados em 2019. Além desse apontamento, o tema foi motivado pelos possíveis impactos causados na sociedade com a implantação da LGPD. Tema que gera grande preocupação nas empresas, uma vez que precisam estar atentas ao cumprimento de regras e ao modo de atuação nos negócios virtuais.

1.3 Materiais e métodos

Como materiais e métodos, este trabalho utilizou de leitura e pesquisa bibliográfica para o levantamento dos conceitos de proteção de dados, dados, informações e direitos individuais de cada cidadão. Além disso foi realizado um breve levantamento entre as leis de proteção de dados vigentes em outros países, como no caso dos EUA, Japão, Argentina e na União Europeia.

Após esse processo, houve a leitura e aprofundamento da lei geral de proteção de dados, trazendo de forma simplificada os artigos descritos na LGPD. Complementando o estudo, foi aplicada a entrevista técnica e estruturada com o objetivo de minimizar alguns pontos levantados durante a pesquisa. Essa entrevista foi aplicada a especialistas no assunto. Para finalização, houve a inclusão da experiência profissional, relatando o momento atual das empresas, bem como o estudo da aplicabilidade e passo a passo realizado por algumas organizações para aderência a lei.

1.4 Objetivo

1.4.1 Objetivo geral

Analisar a lei vigente de proteção de dados pessoais (LGPD) no Brasil e suas implicações na relação entre empresas e usuários no ambiente virtual.

1.4.2 Objetivo específico

Estudar a proteção dos dados pessoais no Brasil, sua relação com a privacidade e os direitos individuais de cada cidadão, trazendo um guia para sociedade Brasileira, com o objetivo de minimizar as lacunas do conhecimento existentes sobre o tema.

1.5 Contextualização do problema

Durante o processo da dissertação, foi realizada uma pesquisa on-line de 11/01/2020 até o dia 15/01/2020. O questionário foi criado a partir da ferramenta Google Forms e liberado em redes sociais como WhatsApp e Facebook. No total, ele foi respondido por 191 pessoas interessadas em proteção de dados, de várias regiões do Brasil e com idade e escolaridade diferentes.

Esta pesquisa trouxe informações relevantes sobre o conhecimento dos indivíduos em relação à proteção de dados, confirmando que o tema ainda não está difundido entre as pessoas. Contudo, é certo que a pesquisa não possui rigor científico, pois a mesma não foi aplicada dentro de uma metodologia de amostragem. A aplicação da pesquisa, utilizando as

ferramentas disponíveis na internet, foi como ponto de partida para validação da importância do assunto e sua relevância social, garantindo assim, a necessidade do tema e as análises que serão apresentadas no decorrer desta pesquisa. Além de apontar a necessidade e a importância sobre o conhecimento das pessoas em relação à proteção dos dados pessoais, investigou-se o perfil dos participantes, considerando a idade, o sexo, a região onde reside, a profissão e o nível de escolaridade, possibilitando uma análise posterior da difusão do conhecimento do tema considerando o perfil dos participantes analisados por regiões, faixa etária e nível de escolaridade.

1.5.1 O questionário de pesquisa

Como será verificado, a aplicação do questionário apontou que a LGPD ainda é desconhecida entre muitas pessoas. Apesar de aparentemente ser uma lei para benefício do cidadão, a mesma não é de conhecimento comum entre a população. As perguntas aplicadas se encontram descritas no Apêndice A.

Para que essa análise fosse possível, as perguntas foram divididas em três categorias: a primeira se refere ao conhecimento do conceito geral sobre proteção de dados, a segunda categoria sobre os dados do próprio cidadão e a terceira categoria direcionada ao entendimento da importância dos dados pessoais para uma organização de informações. Dessa forma, ao preencher o questionário, é possível identificar qual o conhecimento das pessoas sobre as três categorias.

1.5.2 Categoria 1: Conhecimento geral da LGPD

As perguntas que compõem essa categoria são:

- “1. Você sabe o que é proteção de dados pessoais?”
- “2. Você sabe o que é LGPD?”

O objetivo dessa categoria era averiguar o conhecimento das pessoas sobre proteção de dados pessoais e sobre a LGPD. Neste caso, a análise das respostas às perguntas visou identificar o conhecimento das pessoas sobre a proteção de dados, verificando se elas a compreendem como sendo uma forma ou meio de alcançar a privacidade, que é um direito do cidadão, previsto oficialmente em lei.

1.5.3 Categoria 2: Proteção dos dados do indivíduo

As perguntas que compõem essa categoria são:

- “3. Você lê os termos de adesão ou política de privacidade dos serviços que costuma contratar?”
- “4. Na sua opinião, seus dados pessoais estão protegidos?”

Nesta categoria, o objetivo principal era verificar se o próprio indivíduo entende que seus dados pessoais estão protegidos, bem como verificar se eles têm conhecimento da relevância da leitura de termos de adesão e política de privacidade pelo titular dos dados.

1.5.4 Categoria 3: Importância dos dados pessoais para a organização de informações

As perguntas que compõem essa categoria são:

- “5. Para qualquer tipo de aquisição ou utilização de serviços é necessário informar dados pessoais. Você conhece a finalidade de utilização de seus dados para esses serviços contratados?”
- “6. Na sua opinião, seus dados pessoais e interesses são importantes para uma organização/empresa?”

Nesta categoria, o objetivo era entender o conhecimento dos indivíduos sobre a importância de seus dados pessoais e a finalidade de utilização dos mesmos pelas organizações que os exigem.

1.5.5 Validação da pesquisa

Segue abaixo um gráfico com os resultados de todas as perguntas aplicadas na pesquisa on-line realizada com 191 pessoas.

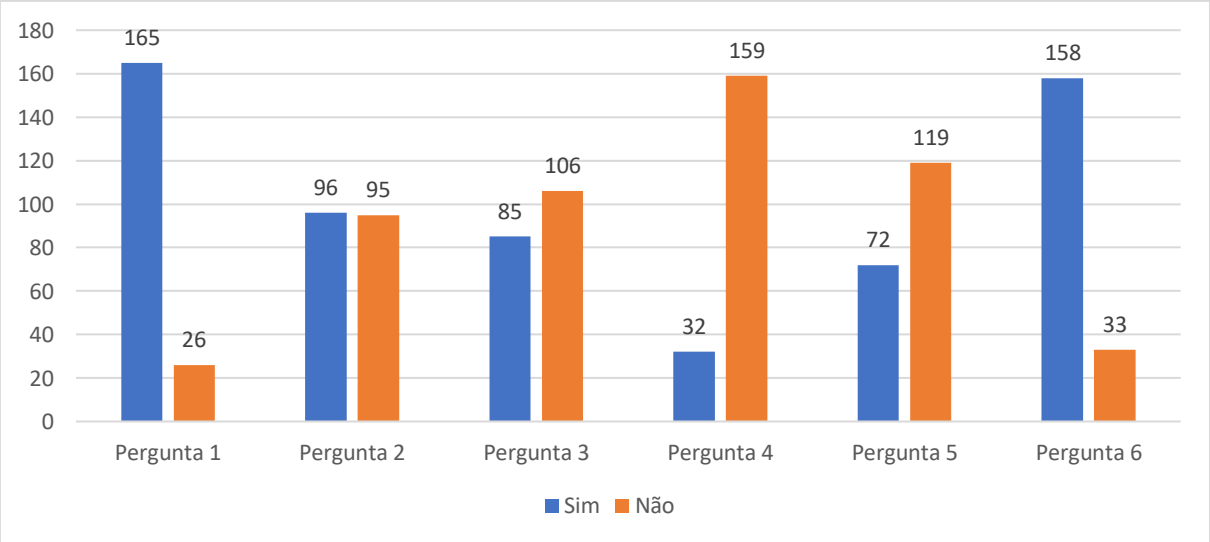


Figura 1 - Respostas do questionário
Fonte: Próprio autor.

A partir da pergunta sobre o conhecimento da LGPD, foi possível verificar que 50,26% conhecem sobre a nova lei, enquanto os 49,73% não conhecem sobre a nova lei. Lembrando que a pesquisa foi respondida com o auxílio de ferramentas digitais e redes sociais, disponíveis em local onde a lei tem maior aplicabilidade e já apresenta alterações relacionadas aos princípios da LGPD.

Foi realizado o agrupamento das pessoas por nível de escolaridade e por idade. Percebeu-se que o aumento do conhecimento da LGPD está relacionado com o aumento do grau de instrução de uma pessoa, ou seja, quanto maior a escolaridade, maior o % de pessoas que conhecem sobre a nova lei. No agrupamento por idade, notou-se que quanto mais jovem, maior o conhecimento sobre a LGPD. Dessa forma, verificou-se que existe o conhecimento maior sobre essa nova lei por parte de pessoas mais novas, de 16 até 30 anos. Dessa forma, com o aumento das faixas etárias, o % de conhecimento da LGPD diminuiu em até 12%.

A seguir, pode ser observada uma tabela com os resultados comparativos, por nível de escolaridade e por idade, separados por grupos.

Por nível de escolaridade		
Ensino Fundamental e Médio		
Conhecem a LGPD	12	26%
Não conhecem a LGPD	34	74%
Total	46	
Graduação		
Conhecem a LGPD	34	57%
Não conhecem a LGPD	26	43%
Total	60	
Pós Graduação		
Conhecem a LGPD	50	59%
Não conhecem a LGPD	35	41%
Total	85	

Por idade		
De 16 até 30 anos		
Conhecem a LGPD	18	64%
Não conhecem a LGPD	10	36%
Total	28	
De 31 até 50 anos		
Conhecem a LGPD	51	53%
Não conhecem a LGPD	46	47%
Total	97	
De 51 até 70 anos		
Conhecem a LGPD	27	41%
Não conhecem a LGPD	39	59%
Total	66	

Tabela 1 - Agrupamento das respostas por nível de escolaridade e por idade
Fonte: Próprio autor.

A pesquisa mostrou que algumas pessoas têm profissões que são altamente impactadas pela LGPD e que, mesmo assim, desconhecem informações do tema. 60% dos Administradores que responderam à pesquisa afirmaram que não sabem o que é a LGPD.

Além deles, 44,44% dos advogados e 12,50% dos empresários também afirmaram desconhecer sobre o tema.

Dentre os participantes da pesquisa, apenas diretores e gerentes, afirmaram conhecer sobre proteção de dados e a LGPD. Dentre esses participantes, todos veem a importância de informar seus dados pessoais para as organizações, porém apenas a metade destes leem os termos de adesão e privacidade quando realizam a contratação de algum serviço ou produto.

Das 159 pessoas que responderam que seus dados não estão protegidos, 58,49% afirmaram que não leem os termos de privacidade e de adesão, ou seja, não possuem o conhecimento da finalidade de utilização dos seus dados pessoais pelas organizações.

Das 119 pessoas que disseram que não conhecem a finalidade de utilização de seus dados, 39,77% afirmaram que leem o termo de adesão. O que podemos aferir que os termos atuais estão escritos de uma forma que gera dificuldades no entendimento do titular dos dados. Além disso, existe o fator de transparência das empresas, onde as pessoas não têm a confiança de que todas as informações estão descritas nos termos disponíveis no ato da contratação de um serviço ou produto.

Ademais, 33 pessoas responderam que acreditam que as empresas não estão interessadas em seus dados pessoais, sendo que dessas pessoas, 87,87% afirmaram que conhecem o que é proteção de dados pessoais.

A partir das respostas do questionário, aumentou a percepção da real necessidade de se compreender a adoção da LGPD pelas empresas e as consequências geradas aos usuários pela não aderência das empresas. A partir disso, houve uma busca dentro dos processos metodológicos e científicos para embasar esta pesquisa, trazendo conceitos sobre a proteção de dados e informações a respeito da LGPD, possibilitando aos cidadãos que se beneficiem com o conteúdo desta pesquisa.

CAPÍTULO 2: PRIVACIDADE E VIOLAÇÃO NO USO DOS DADOS PESSOAIS

Neste capítulo será apresentado sobre a transformação de dado em informação, técnicas de mineração de dados e suas etapas, a utilização das informações pelas organizações públicas e privadas, além do dado como um direito individual, ressaltando os conceitos de proteção e violação de dados pessoais.

2.1 Dado x informação x conhecimento

Para contextualizar esta pesquisa, é importante o estudo de três tópicos que estão atrelados ao tema em discussão e que juntos são capazes de gerar valor a ser observado e considerado na relação empresas e usuários: o conceito de dado, a informação e o conhecimento. Para Guimarães (20--), **dado** é o conhecimento bruto ou matéria prima da informação que ainda não foi tratada e não gerou nenhuma informação relevante ao negócio. Castro (2011) afirma que **dado** pode ser definido como uma sequência de quantificados ou quantificáveis que ainda não possui uma inteligibilidade à informação. Um dado pode ter uma infinidade de definições que depende da ciência que o cerca. Dessa forma, para esta pesquisa será considerado que um **dado** é uma **informação** em sua forma simples, sem um processamento que o torna relevante. Guimarães (20--) explica que a informação é o dado devidamente tratado que produziu um conhecimento relevante à organização. Castro (2011) explica que a **informação** é vista como um estímulo a um determinado dispositivo, agrupado em padrões que influenciam a transformação de outros padrões, sem que a mente o reconheça tal como padrão. Em linhas gerais, a informação é a transformação de um dado em padrões que geram um valor.

Abaixo, uma imagem demonstrando o processo de transformação de um dado em informação.

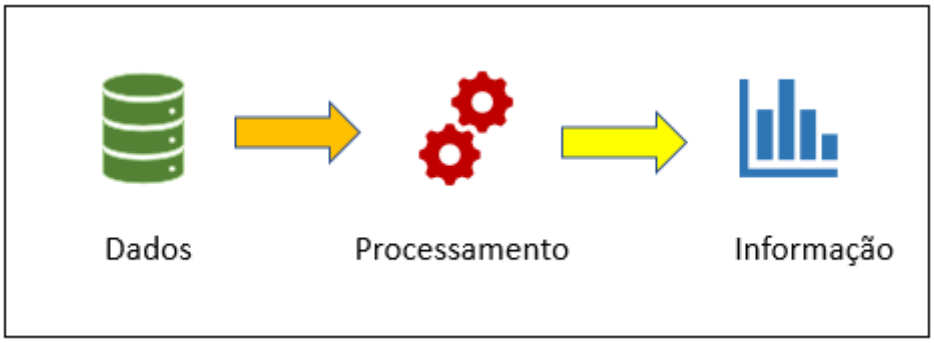


Figura 2 - Processo de transformação de dado em informação
Fonte: Próprio autor.

Conforme o dicionário on-line Dicio (2021), **conhecimento** é definido como a ação de entender por meio da inteligência. Nessa linha de raciocínio, a partir de uma coleta básica de um dado, é possível transformá-lo em informações processadas, agrupando em padrões pré-estabelecidos. Assim, o conjunto de informações agregados a inteligência torna-se o conhecimento.

Essas definições ajudam no entendimento da importância das informações para as organizações, que buscam incansavelmente por dados para usá-los no processo decisório no curso das empresas e para a prospecção de novos negócios a partir do conhecimento gerado com os dados dos usuários. Entende-se que qualquer tipo de dado de indivíduo seja importante para esse processo contínuo dentro das organizações, possibilitando a retroalimentação das informações dentro do sistema corporativo.

Com o passar do tempo, os dados coletados e as informações tratadas criam um alto custo operacional e tecnológico para as organizações, que armazenam milhares de informações por um longo período de tempo. Além disso, com o crescimento dessas informações, aumenta-se a dificuldade na extração dos dados. Diante desse cenário, o processo de mineração de dados, torna-se uma ferramenta importante para as organizações. No próximo item, será descrito sobre esse processo.

2.2 Mineração de dados (*data mining*)

Para Bortoli (2012), mineração de dados consiste em um processo analítico e projetado para explorar grandes quantidades de dados na busca de relacionamentos sistemáticos entre variáveis. Dessa forma, é possível afirmar que a mineração de dados prevê o processamento de dados simples, unindo e cruzando esses dados para que sejam transformados em uma informação relevante para o processo decisório.

A figura a seguir demostra o processo de mineração de dados, onde os dados funcionam como entrada deste processo, que filtra as informações relevantes. O processo de mineração de dados funciona como um funil, no qual permanecem após o processamento apenas informações que possibilitam a padronização, ou a classificação, e que possuam relevância para o negócio.

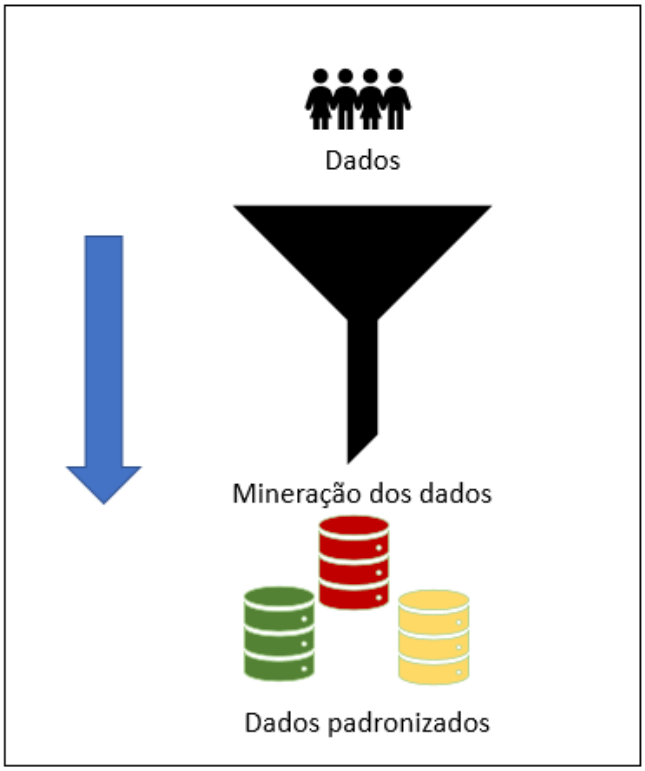


Figura 3 - Processo de mineração de dados
Fonte: Próprio autor.

Há anos empresas estão procurando tendências para seus negócios por meio de técnicas como a mineração de dados. O processo de minerar dados para descobrir conexões escondidas e prever tendências iniciou-se com o método chamado "descoberta de conhecimento em bancos de dados", de acordo com o *site* SAS (20--). O termo "mineração" só foi utilizado nos anos 1990, mas sua base compreende três disciplinas científicas entrelaçadas que existem há tempos: estatística (o estudo numérico das relações entre dados), inteligência artificial (aquela exibida por *softwares* e/ou máquinas, que se assemelham à inteligência humana) e *machine learning* (algoritmos que podem aprender com dados para realizar previsões), expõe o *site* SAS (20--). Observando o comportamento diário das pessoas, toda a análise é feita por meio da observação, seja do comportamento ou de características físicas, traçando caminhos, através do conhecimento adquirido durante toda a vida.

Conforme SAS (20--), a tecnologia de mineração de dados continua evoluindo para acompanhar o potencial ilimitado do *big data*[3] e a computação de baixo custo. Conclui-se assim que cada vez mais se torna possível o processamento de uma quantidade maior de

[3] **Big Data** é um termo utilizado pela área de tecnologia da informação referente ao grande conjunto de dados. Fonte: Cetax (2020).

informações com menor tempo e custo, trazendo um nível de assertividade e velocidade maior para as organizações que investem no processo de mineração de dados.

Varejistas, bancos, fabricantes, operadoras de telecomunicações, seguradoras entre outras estão usando a mineração de dados para descobrir relações que podem ser estabelecidas a partir de vários aspectos de suas organizações, como preços, promoções, demografias, economia, risco e principalmente concorrência. Essa prática de mineração de dados tem afetados seus modelos de negócios, receitas, operações e relacionamentos com os clientes, por meio das mídias sociais, afirma o *site* SAS (20--).

Para o *site* Rockcontent (2020), a mineração de dados colabora com a análise do comportamento dos clientes e concorrentes, possibilitando a antecipação de demandas, trazendo grandes benefícios para a empresa. Com toda essa tecnologia disponível, o processamento dos dados ficou muito mais simples e rápido, com um custo operacional e sistêmico cada vez menor em comparação aos benefícios trazidos com as análises eficientes criadas nas organizações e geradas pelo processo de mineração de dados.

2.2.1 Etapas da mineração de dados

Bortoli (2012) afirma que o processo é basicamente formado de 3 etapas: exploração, construção de modelo ou definição do padrão e validação/verificação. Já para o *site* Rockcontent (2020) o processo de mineração de dados é composto de cinco etapas que precisam interagir entre si, de modo que a primeira etapa está relacionada à definição do problema, a segunda, à redução de dados duplicados e redundantes, a terceira, à exclusão de pontos irrelevantes ao objetivo final estabelecido na primeira etapa, a quarta, à limpeza dos dados, e por último a mineração de dados, etapa na qual se identificam os padrões que podem ser utilizados pela empresa ou organização.

Muitas são as divergências sobre as etapas do processo de mineração de dados, porém impendente dos nomes de cada uma dessas etapas, é possível considerar em linhas gerais que o processo de mineração de dados consiste em identificar inicialmente quais os dados relevantes para o processo, agrupar as informações e transformá-las em um padrão mais limpo e fácil de ser processado. Dessa forma, ao iniciar a mineração de dados, é necessário analisar os objetivos finais, ou seja, quais informações serão necessárias para a organização/instituição, além de verificar quais análises e relatórios serão importantes. Partindo desse levantamento, identifica-se os dados que são relevantes para o objetivo final, todo o restante é descartado. Após esse descarte, os dados relevantes são agrupados em

padrões pré-estabelecidos. Muitas vezes, durante esse agrupamento, realiza-se o armazenamento das informações já processadas.

Para facilitar o entendimento sobre o processo de mineração de dados, segue exemplo: uma base de dados contém todos os acessos e ações dos usuários em um sistema. O objetivo final da mineração de dados está na extração das informações conforme tendências do comportamento dos usuários. Dessa forma, como os dados que serão extraídos estão relacionados à tendência, não existe a necessidade de armazenar o nome dos usuários, portanto esse dado será descartado. Feito o descarte dessa informação, os *logs* de acessos serão processados e transformados em uma única linha com a quantidade de acessos e as ações realizadas em cada parte do sistema. Portanto, após o processo de mineração de dados, houve uma diminuição significativa na quantidade de informações. Elas deixam de ser analíticas e passam a ser sintéticas. O processo de mineração de dados também diminui o armazenamento em bancos de dados, reduzindo os custos de hospedagem e a infraestrutura necessárias para suportar grandes informações.

2.3 Oversharing

O chamado *oversharing*, definido por Freire (2015) como compartilhamento sem limites dos dados pessoais nas plataformas de mídia na Internet, tem se intensificado com a exposição acelerada dos internautas, compartilhando cada vez mais sua vida particular e dados sensíveis em plataformas digitais. Conforme o *site* Sbie (2016), a palavra *oversharing* é formada pela junção dos termos "*over*", que significa excesso, e "*sharing*", que significa compartilhamento. O *site* complementa que este conceito é aplicado quando diz respeito ao compartilhamento exagerado de fotos, pensamentos, pontos de vista, ações ou até mesmo fatos irrelevantes na internet. Este "supercompartilhamento" se intensificou com a utilização em massa dos dispositivos móveis, aos quais se tem mais acesso atualmente, devido ao crescimento da classe consumidora desses dispositivos, favorecida ainda pelo barateamento do acesso à Internet, facilitando cada vez mais que as emoções sejam extravasadas. Conforme Staudt (2017), todos os sentimentos e a busca de uma vida perfeita se tornaram realidade no mundo virtual, o que atraiu e atrai, cada vez mais, seguidores e utilizadores dessas plataformas sociais. Muitas vezes, os dados disponibilizados de forma aleatória, não oferecem risco, mas após seu processamento, é possível criar verdadeiros arquivos de informação, com os dados mais diversos a respeito do comportamento social, econômico e pessoal de um indivíduo, afirma Hirata (2014). Muitas pessoas realizam muitos compartilhamentos em redes sociais, porém não utilizam aplicativos bancários e não realizam

compras on-line, pois não sentem segurança em ter seus dados bancários expostos. É possível perceber que as pessoas, principalmente os mais idosos, têm medo da internet no âmbito financeiro, mas não percebem o risco nos excessos de compartilhamento sobre os dados pessoais e principalmente dados sensíveis. Porém, ao longo do tempo, esses números estão mudando, conforme pesquisa da Febraban (2019) de cada 10 transações bancárias no Brasil, seis já são realizadas pelo celular ou computador. O crescimento das transações e da confiabilidade do digital vem aumentando a cada ano, conforme pesquisa do setor financeiro. Esse aumento deve-se principalmente pelo alcance da tecnologia em várias regiões e pelo crescimento populacional de uma geração que já nasceu conectada à internet.

2.4 As informações como estratégia global das empresas

Para as tomadas de decisões, as organizações utilizam de informações. Chiavenato (2000) afirma que os antepassados passavam a maior parte do tempo buscando encontrar energia ou informação para dirigir suas organizações. Historicamente, a utilização dos dados sempre ocorreu para a tomada de decisões juntamente com a dificuldade em encontrá-las e processá-las. O processamento dessas informações, no passado, era realizado de forma manual, sendo possível uma análise com base em poucas informações, no entanto, essa situação torna o resultado menos assertivo e o processo, lento.

Segundo Teixeira Filho (2000), o conhecimento é usado de forma não explícita nas organizações, por trás das milhões de decisões estratégicas e operacionais, ao longo dos anos. O autor complementa que essas informações eram transmitidas de pessoas para pessoas, através de meios estruturados como livros, vídeos, documentos e etc. Com o passar do tempo, a informação se consolidou e tornou-se ainda mais relevante, e seu processamento possibilitou decisões assertivas. Conforme Costa (2018), o conhecimento e a informação tornaram-se um aspecto relevante na sociedade moderna. O *site* Impacta (2019), comenta que atualmente diversas empresas utilizam dados para monitoramento do perfil de um público especifico e extrai *insights* para o negócio. No momento atual, com todo o contexto tecnológico disponível, a sociedade criou um cardápio de informações atrativas para as empresas, organizações, governos e outros órgãos que estão em busca de conhecer o indivíduo e tomar cada vez mais, decisões que trazem resultados satisfatórios. Esse cardápio, criado a partir do ato do compartilhamento desenfreado da sociedade que busca comodidades através do digital, possui crescente presença nas redes sociais, em *sites* de compra e em busca por materiais digitais. Isso torna os indivíduos cada vez mais vulneráveis, pois disponibilizam uma enorme quantidade de dados que são captados em forma de troca e sem um prévio conhecimento de

sua utilização. As principais formas conhecidas atualmente para a captação de dados pelas empresas ou organizações estão relacionadas ao acesso às redes sociais, à captação através de formulários em troca de conteúdo, à compra de dados e aos dados históricos existentes na própria empresa.

No caso das redes sociais, os indivíduos compartilham e publicam sobre sua vida pessoal e sobre os seus interesses. Conforme Vieira (2020), alguns algoritmos próprios de leitura de conteúdo de redes sociais são capazes de interpretar essas informações aleatórias segmentando-as e priorizando-as em conteúdo relevantes. Dessa forma, os dados publicados pelos usuários de forma espontânea, passam por um processamento, transformando as características e interesses relacionados à pessoa em um perfil comportamental e social que tem valor ao mercado.

Já a captação com base em respostas informadas em formulários em troca de conteúdo funciona como uma isca. A empresa ou organização desenvolve um conteúdo atrativo ao público que deseja alcançar, porém para que esse público tenha acesso ao conteúdo na integra é necessário o preenchimento das informações pessoais. Essas informações podem ser utilizadas para diversas finalidades, como o envio de promoções e propagandas ou até mesmo a criação de uma base para o funil de vendas.

Outra forma conhecida, porém menos divulgada, é a compra de dados. Existe um comércio no qual dados pessoais, como número de telefone, nome e *e-mail* são previamente categorizados e vendidos para empresas que estão em busca de novos *leads* ou de informações para tomada de decisões.

Por último, tem-se as bases existentes dentro da própria organização. Cadastros de clientes ou de pessoas que já foram clientes são mantidos em posse das empresas ou organizações que os utilizam para diversas finalidades comerciais. A partir do processando dos dados históricos, os mesmos são transformados em arquivos importantes para decisões futuras dentro da organização.

2.5 Dados como direitos individuais

Questões relacionadas à proteção dos dados são levantadas constantemente, como os vazamentos de dados que são frequentemente noticiados. Muitos especialistas e noticiários comentam sobre esse assunto e cada vez mais estão preocupados com as questões da coleta de dados e a utilização indevida destes pelas organizações, que não garantem à privacidade dos indivíduos. Oliveira *et al*. (2019) afirma que o desdobramento da privacidade é um efeito colateral da mudança de paradigma trazida pela “Quarta Revolução Industrial”, devido ao

fenômeno da “informacionalização da sociedade”, iniciado na década de 1970. Com a sociedade informatizada, os dados precisam da proteção necessária, garantindo assim os principais direitos de cada indivíduo. Direitos estes, previstos na Constituição Federal de 1988, art5, inciso X:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 2020).

A proteção de dados deve ser pensada durante todo ciclo de vida de um dado e está relacionada às informações disponibilizadas pelos próprios usuários. Dessa forma, existe a preocupação relacionada à proteção de dados versus o direito individual do cidadão em escolher quais informações relacionadas a ele deseja compartilhar. Muitas vezes, essas informações são compartilhadas sem o conhecimento dos titulares de dados, pois não conhecem os riscos oferecidos à sociedade como um todo ao divulgar seus próprios dados.

Oliverira *et al*. (2019, np) afirma que:

> (...) um longo percurso histórico teve de ser percorrido até que a privacidade pudesse ser reconhecida como um bem jurídico digno de tutela Estatal.

Fugazza e Saldanha (2017) complementam que as pessoas estão inseridas em uma cultura que favorece a transparência, porém, ao mesmo tempo, não existe garantia da proteção da privacidade dos indivíduos no ambiente digital. Para a autora, isso constitui um dilema central que está presente no mundo contemporâneo. O dilema central, que foi observado por Fugazza e Saldanha (2017), foi minimizado com a nova LGPD, porém mesmo que ela já esteja em vigor, as questões de privacidade ainda levantam muitas discussões.

A nova LGPD, publicada em agosto de 2018, mas que entrou em vigor em 18 de setembro de 2020, trouxe novos desafios para praticamente toda as empresas. Oliveira *et al*. (2019) afirmou que, até a entrada em vigor da LGPD, as pessoas naturais e jurídicas que estejam sob sua abrangência deveriam se adequar às novas exigências legais. Porém, as empresas ainda trabalham incansavelmente para atingir total abrangência das exigências da lei, sendo possível verificar que os impactos dentro das empresas não foram cessados.

2.6 Proteção de dados

A proteção de dados pessoais tornou-se um tema de preocupação mundial devido à quantidade de vazamentos de dados que vem crescendo muito nos últimos anos, e é notícia constante em meios de comunicação.

Conforme definição apresentada por Zeferino (2020), o termo **proteção de dados** tem um significado muito amplo, porém é comum ele estar ligado à terminologia jurídica.

É possível considerar a proteção de dados como um meio para garantir a proteção aos dados de um cidadão, que utiliza medidas técnicas e organizacionais, referindo-se a um direito fundamental da pessoa. A proteção de dados cria meios para garantir que os dados apenas sejam tratados para as finalidades aprovadas previamente pelo titular dos dados. Dessa forma, o termo proteção de dados está relacionado com a definição de processos que padronizem os tratamentos de dados pessoais, evitando falhas e violações durante todo o ciclo de vida dos dados na organização. Diante desse cenário, é dever do responsável pelo tratamento de dados implementar tais medidas técnicas e organizacionais, garantindo assim que os direitos do titular dos dados sejam respeitados durante a utilização dos dados pela organização.

Conforme a Lei geral de proteção de dados, Artigo 2, a disciplina de proteção de dados pessoais tem como fundamento:

> Art. 2º A disciplina da proteção de dados pessoais tem como 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. (BRASIL, 2018, np.)

O processo de proteção de dados inicia com os dados fornecidos pelo titular dos dados. Dentro da organização esses dados são armazenados em banco de dados ou arquivos onde serão aplicadas medidas técnicas, ou seja, processos, para garantir a proteção desses dados. A seguir, a figura apresenta uma imagem sobre o processo de proteção de dados dentro das empresas ou organizações,

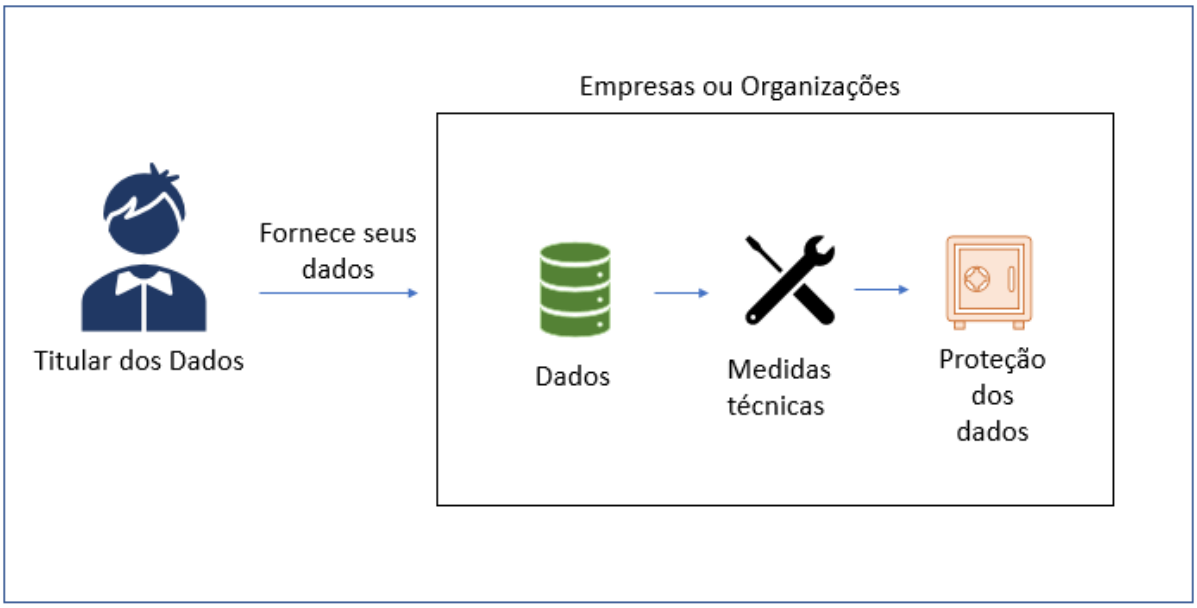


Figura 4 - Proteção de dados
Fonte: Próprio autor.

2.7 Violação de dados pessoais

Toda violação de dados pessoais começa com uma vulnerabilidade de sistemas ou processos. A vulnerabilidade representa uma brecha ou falha existente dentro de uma organização que pode vir a ser explorada. Ela torna-se um incidente de segurança quando os dados efetivamente ficam expostos, porém é importante ressaltar que, mesmo com a exposição dos dados, pode não ocorrer a violação deles, pois um incidente de segurança nem sempre significa que os dados foram acessados por pessoas ou organizações sem a autorização devida. Quando os dados expostos caem em mãos de pessoas mal-intencionadas ou são apagados sem autorização e sem chance de recuperação, ocorre então uma violação de dados. No momento em que esses dados violados são pessoais, é possível afirmar que ocorreu uma violação de dados pessoais. Conforme Garrute e Schmidt (2020), tanto o acesso sem a devida autorização a dados pessoais quando a divulgação não autorizada desses dados são considerados uma violação aos dados pessoais. Por exemplo, um servidor danificado por um raio permite que os dados de milhares de usuários sejam perdidos. Caso a empresa não tenha um *backup* para recuperar os dados, podemos considerar que houve uma violação de dados pessoais. Porém, se foi possível a recuperação destes dados, é possível afirmar que tudo não passou de um "incidente de segurança".

A figura a seguir mostra o processo de violação de dados pessoais.

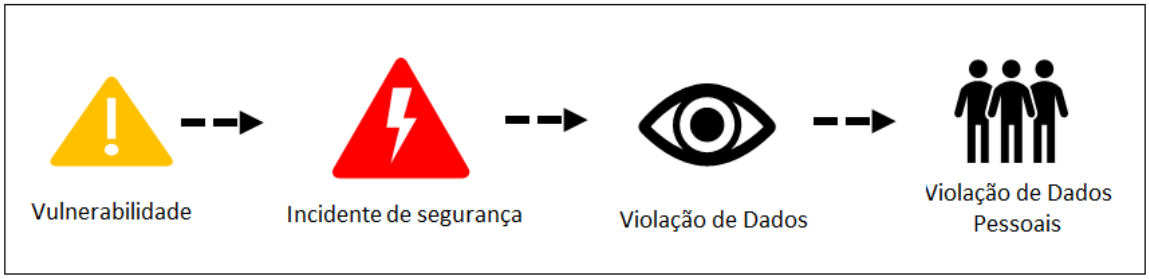


Figura 5 - Fluxo da violação de dados pessoais
Fonte: Próprio autor.

Garrute e Schmidt (2020) apontam que, de acordo com o artigo 4(12) do GDPR, a violação de dados pessoais consiste em:

> (...) uma infração da segurança que tenha por efeito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, seja de modo acidental, seja de modo ilícito. (GARRUTE; SCHMIDT, 2020, np.).

2.7.1 Categorias de violação de dados pessoais

A violação de dados pode ser categorizada para facilitar o entendimento das formas de violação. As categorias vão além de uma invasão por *hackers* em um servidor, muitas vezes elas ocorrem dentro do próprio ambiente corporativo pelas pessoas que manipulam esses dados. Essas categorias são definidas como: material, verbal e não material e digital.

A seguir, a figura demonstra as categorias de dados pessoais.

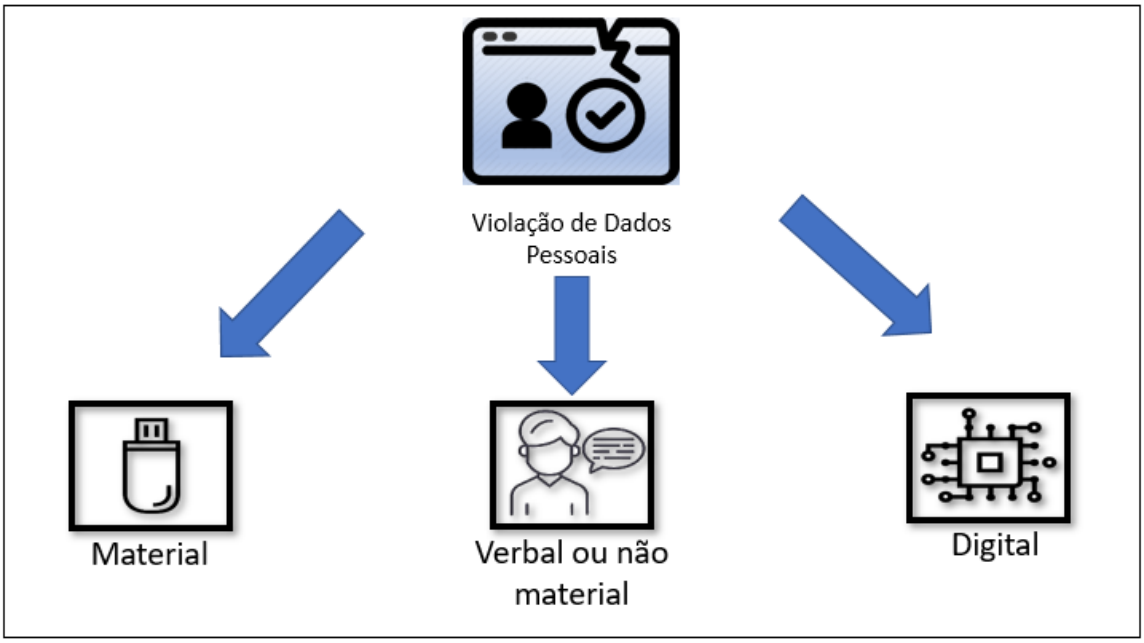


Figura 6 - Categorias de violação de dados pessoais
Fonte: Próprio autor.

Abaixo, seguem imagens com a descrição de cada categoria de violação de dados pessoais: material, verbal e não material e digital.

2.7.1.1 Material

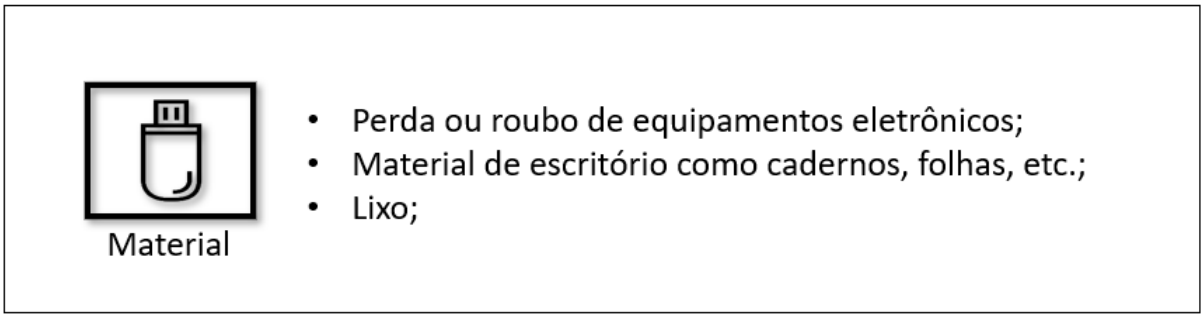


Figura 7 - Violação de dados material
Fonte: Próprio autor.

A categoria de violação de dados material abrange todas as ameaças físicas que contenham informações pessoais de algum titular de dados. Nessa categoria, é enquadrado qualquer tipo de perda ou furto de equipamentos eletrônicos como *notebook*, celular entre outros. Além disso, também faz parte dessa categoria, a perda ou o furto de materiais de escritório não digitais, como cadernos, folhas, arquivos entre outros.

Macêdo (2017) comenta sobre uma forma de ameaça relacionada ao lixo gerado por uma pessoa, o chamado *Dumpster Diving*. A partir do lixo gerado em casa, informações importantes e sensíveis sobre uma pessoa podem ser coletadas. Muitas vezes, o lixo não demonstra um risco, porém após ser processado e separado pode apresentar informações sobre os costumes e hábitos de uma pessoa ou de uma família a pessoas ou organizações não autorizadas.

2.7.1.2 Verbal ou não material

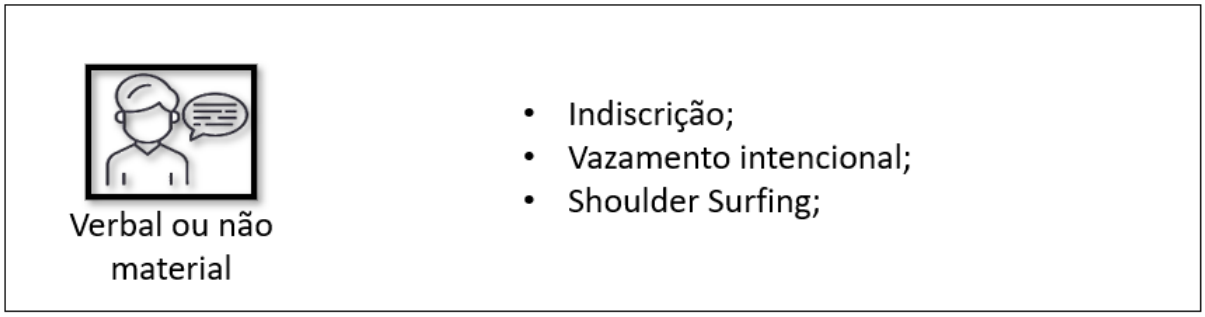


Figura 8 - Violação de dados verbal e não matéria
Fonte: Próprio autor.

Na categoria verbal ou não material, considera-se a ocorrência das violações de dados de forma verbal, através da fala, ou comunicação verbal entre as pessoas. É considerada violação de dados verbal, a utilização da indiscrição ou o vazamento intencional de dados, ou seja, a transmissão de dados por meio de fofocas proferidas por pessoas que detêm o acesso aos dados pessoais, passando essas informações a outras pessoas que não deveriam ter acesso a essas informações. Qualquer comunicação verbal informal, em que o receptor não tem acesso às informações, é considerada uma indiscrição. Para minimizar esse tipo de violação e aumentar a proteção de dados, é importante que as empresas solicitem aos seus colaboradores a assinatura de um contrato de NDA ("*Non Disclosure Agreement*"), a partir do qual concordam em manter confidencial certas informações. De acordo com o *site* BLB Brasil (2019), NDA significa na tradução livre um acordo de não divulgação, ou seja, um acordo para garantir que as partes mantenham dados confidenciais em sigilo, conforme conceitos, processos, produtos e serviços que ficam resguardados pelo acordo.

Outra forma de violação de dados dentro dessa categoria é o "*shoulder surfing*", termo em inglês relacionado ao *surf* de ombro. Com base da definição desse termo, entende-se que é possível espionar por cima dos ombros informações que estão sendo tratadas por uma pessoa que tem acesso a esses dados e sejam vistas por pessoas não autorizadas. Macêdo (2017) define esse termo como a capacidade de uma das partes de olhar sobre o ombro de outra pessoa.

2.7.1.3 Digital

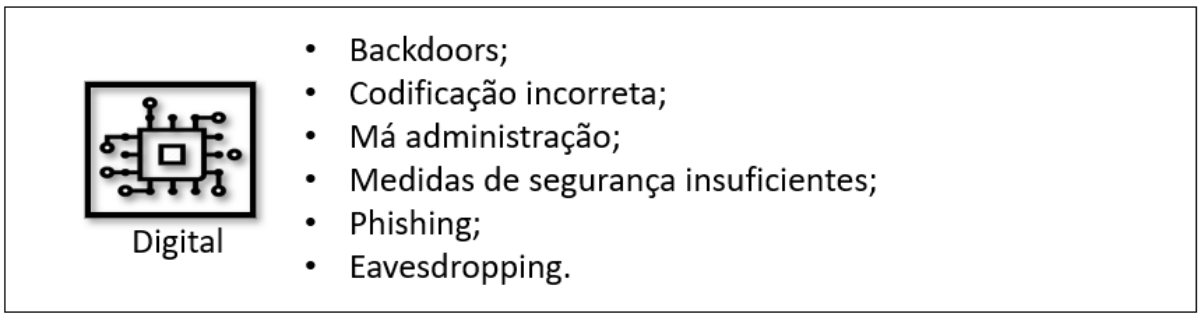


Figura 9 - Violação de dados digital
Fonte: Próprio autor.

Na categoria digital, são consideradas todas as formas de violação de dados realizadas por meio de mecanismos digitais. Os *backdoors* são portas de entrada dentro de uma organização e o maior perigo existente nas empresas atualmente. Essas portas são abertas no momento que um usuário recebe um *e-mail*, aparentemente legítimo, para atualização de

dados cadastrais, por exemplo, e ao clicar para atualizar esses dados, arquivos são instalados na máquina do usuário, abrindo portas para ataques de *hackers*. Em um ambiente onde tudo está interligado pela rede, a porta fica aberta para acesso a informações presentes em toda empresa e não somente para acesso a um único computador.

Ainda na categoria digital, são conhecidas também as codificações incorretas que contemplam os erros no desenvolvimento do *software*, criando falhas e brechas para invasões de pessoas e *softwares* com más intenções. Complementando a codificação incorreta e a tornando cada vez mais perigosa, ressalta-se a má administração ou medidas de segurança insuficientes que tornam o ambiente cada vez mais vulnerável. A má administração e as medidas insuficientes estão ligadas com a falta de investimento em tecnologia para prevenção de riscos em redes, como a atualização de antivírus ou *firewalls*. A área de infraestrutura de tecnologia nem sempre é bem vista por gerar um custo alto de atualização e nenhum retorno imediato para a empresa, o que muitas vezes não é priorizado pela administração, gerando danos gigantescos caso ocorra uma invasão.

Phishing funciona como uma verdadeira pescaria, segundo informado pelo *site* Malwarebytes (20--). A utilização dessa técnica possibilita a captação de dados confidenciais, através de *e-mails* fraudulentos, que imitam os verdadeiros, enganando assim as pessoas que o recebem.

E por último o *Eavesdropping*, termo em inglês, que se refere à espionagem, como atitudes de ouvir conversas ao telefone, acessar conversas no celular, entre outras formas de espionagem realizada por *hackers*.

CAPÍTULO 3: A LEI PARA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Neste capítulo será estudado sobre a Lei geral de proteção de dados, iniciando com uma explanação sobre os dados pessoais. Posteriormente será analisada a estrutura da LGPD, detalhando as partes envolvidas, as bases legais, os princípios legais para tratamento dos dados pessoais e os direitos dos titulares de dados. A finalização desse capítulo abrange a forma em que as empresas e as pessoas poderão agir no caso de uma possível violação de dados pessoais.

3.1 O que é a LGPD?

A sigla LGPD representa o termo Lei geral de proteção de dados, lei Nº 13.709, de 14 de agosto de 2018, que entrou em vigor em 18 de setembro de 2020. A LGPD é análoga à GDPR (*General Data Protection Regulation*) da União Europeia que está em vigor desde 25 de maio de 2018.

Conforme o *site* Ideação (2019) a União Europeia é conhecida por aplicar padrões de proteção de dados pessoais, além das medidas e sanções rigorosas. Com a entrada da GDPR em vigor, muitos países se viram na necessidade de estabelecer medidas e políticas de proteção de dados para que fosse possível a comercialização de produtos e serviços com países da União Europeia, visto que a GDPR só permite a contratação de atividades entre países que possuem uma lei de proteção de dados em vigor. Com o cenário da UE, o presidente da república em exercício na época, Michel Temer, sanciona a chamada Lei geral de proteção de dados, em 14 de agosto de 2018, complementando o Marco Civil da Internet de 2014. Para Gogoni (2018), a LGPD é uma reação a GDPR, já para o Soares (2019), a LGPD buscou inspiração na GDPR.

Vale ressaltar o objetivo principal da LGPD, conforme apresentado na Lei nº 13.709.

> Esta Lei 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. (BRASIL, 2018, np.).

Na prática, a LGPD foi criada para proteger a privacidade das pessoas físicas, para que os dados pessoais dos titulares não sejam furtados ou utilizados de forma não transparente por terceiros, situações em que a lei se aplica. Para Ramos (2020), o grande acerto da LGPD está na criação de uma cultura de zelo e cuidado sobre a privacidade de dados. Apesar do nome da

lei não conter a palavra pessoal, ela apenas se refere aos dados pessoais, aplicando-se à pessoa natural ou jurídica, pública ou privada, que realize tratamento de dados pessoais, ou seja, que exerça atividade em que se utilizem dados pessoais (coleta, armazenamento, compartilhamento, exclusão etc.), independentemente do meio de tratamento, abrangendo também formas de tratamentos não digitais, porém apenas para fins comerciais. Nesse sentido, ela é aplicada a operações de tratamento realizados no Brasil, ou quando houver oferta de bens e serviços para indivíduos localizados no Brasil, ou ainda para dados coletados dentro do território brasileiro. A LGPD não se aplica para dados provenientes e destinados a outros países, que apenas transitem pelo território nacional, para uso pessoal, para uso não comercial, para fins jornalísticos, artísticos, acadêmicos ou de segurança pública. Com a vigência da LGPD em 2020, muitas empresas sofreram e ainda sofrem o grande impacto causado para a adaptação das novas regras. Com isso, houve a necessidade de uma mudança cultural que começa a ser promovida nas empresas para atingir a conformidade com a lei.

> Os impactos desta nova norma são expressivos, tanto no aspecto da tutela da privacidade e proteção dos dados pessoais de seus respectivos titulares, quanto, naturalmente, para a atividade empresarial, considerando que a LGPD impõe uma série de diretrizes para que o tratamento de dados seja realizado de forma lícita. (OLIVEIRA *et al*. 2019, np.).

3.2 Dados pessoais

A LGPD refere-se apenas ao tratamento dos dados pessoais, por esse motivo, é necessário definir o que são dados pessoais. Os dados pessoais são considerados qualquer tipo de informação que possa levar à identificação de uma pessoa, de maneira direta ou indireta. Dados pessoais diretos são dados que não precisam de nenhum processamento para identificação do indivíduo, como o nome, o número do RG, ou do CPF. No caso de dados pessoais indiretos, a identificação do indivíduo dependente da junção das informações coletas com outras, ou seja, a partir de um processamento, como o número da placa de um carro que, com a junção dos dados cadastrais presentes no DETRAN, torna possível a identificação da pessoa física a qual tem a posse do veículo cadastrado sobre o número da placa em questão.

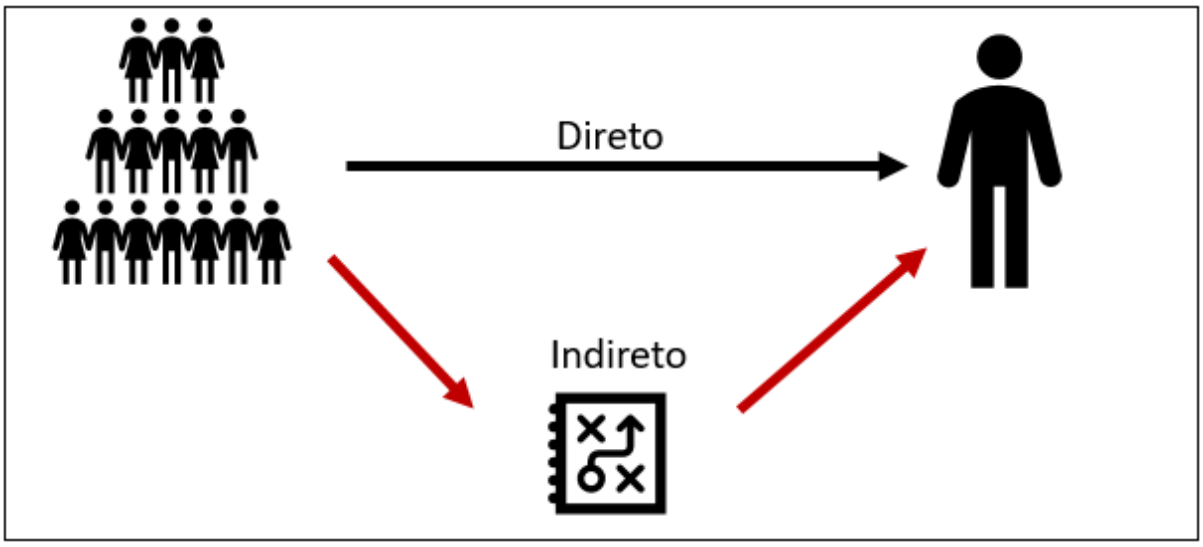


Figura 10 - Identificação de dados pessoais de forma direta ou indireta
Fonte: Próprio autor.

Outros exemplos de dados pessoais são: o endereço de IP de uma máquina, o endereço residencial, *cookies*[4], lista de compras do mercado entre outros.

A lei trata de forma diferente duas categorias principais de dados pessoais. Essas categorias precisam de mais atenção em seu tratamento e no caso de posse desses dados é importante que os mesmos sejam tratados de forma diferente e com mais cuidado. Essas categoriais especiais estão relacionadas com os dados de menores de 18 anos e os dados considerados sensíveis pela lei. Abaixo, o detalhamento de cada um deles.

3.2.1 Dados pessoais de menores de 18 anos

Os dados pessoais de menores de 18 anos devem ser tratados apenas com o consentimento explícito dos pais, para os fins necessários. A lei define que, quando houver dados de menores, se faz necessário o consentimento dos pais ou do responsável legal do menor. Para tanto, a lei informa que o controlador dos dados deve realizar todos os esforços razoáveis para a captação desse consentimento e para a verificação de que ele foi dado realmente por um responsável legal do menor. Em alguns casos, dependendo da base legal de tratamento desses dados, mesmo sem o consentimento do responsável legal, pela lei é possível realizar o tratamento desses dados. Por exemplo, há alguns casos, como por motivo da tutela em saúde, que mesmo sem o consentimento dos pais existe uma base legal, na qual o consentimento deve ser desconsiderado, podendo dessa forma realizar o tratamento dos dados

[4] ***Cookies*** são pequenos arquivos criados por *sites* visitados e que são salvos no computador do usuário, por meio do navegador. Fonte: Alves (2018).

do menor, garantindo o bem estar e a saúde da criança e do adolescente. É possível, no entanto, coletar os dados do menor, juntamente com o contato dos pais, para posteriormente requisitar o consentimento, como mostra a imagem do processo de captação dos dados do menor de 18 anos, solicitando posteriormente o consentimento do responsável legal.

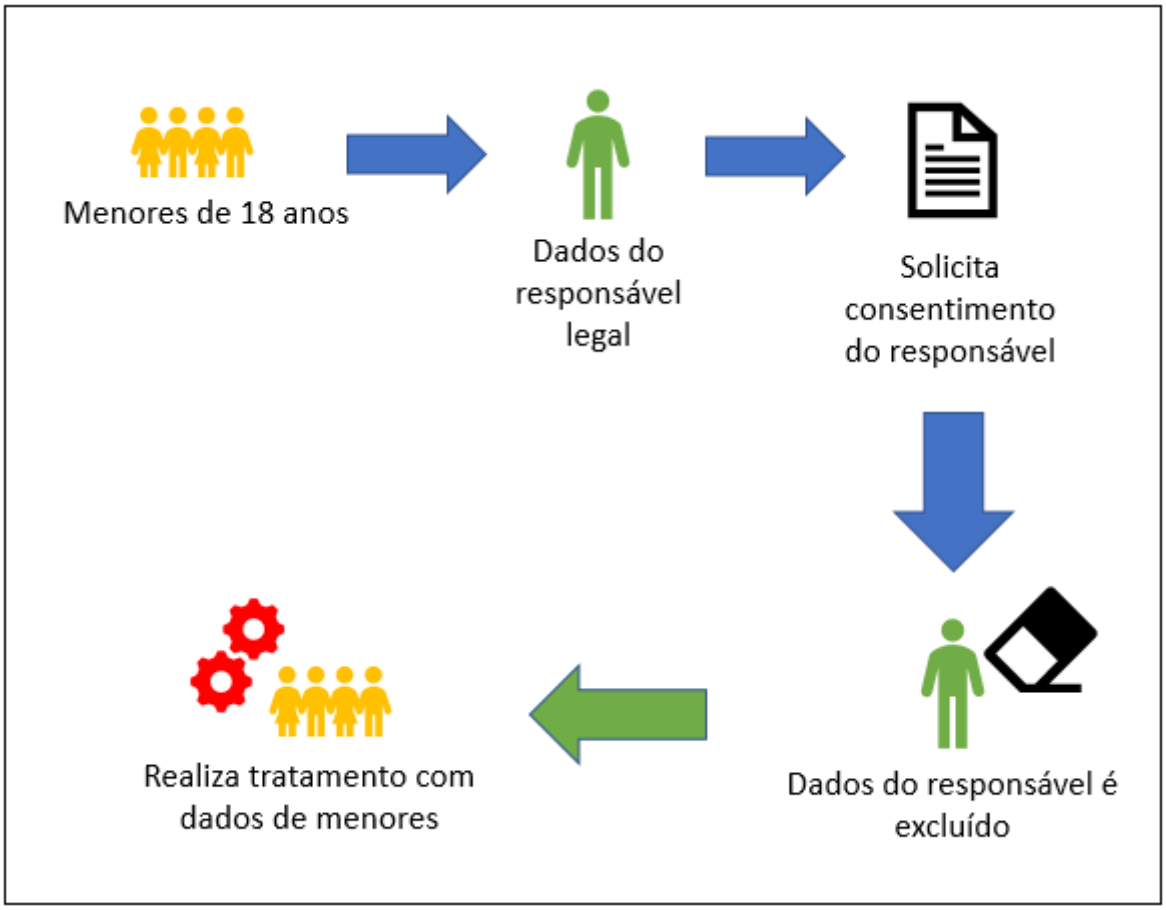


Figura 11 - Processo de consentimento de menores de 18 anos
Fonte: Próprio autor.

3.2.2 Dados pessoais sensíveis

Esta é uma categoria especial de dados pessoais, exigindo mais cuidado por parte do controlador/operador. Essa separação nos dados existe porque entende-se que os dados sensíveis podem causar um prejuízo ou grande impacto à vida e à liberdade do titular dos dados, gerando a ele discriminação ou perseguições, sendo necessário em alguns casos, por exemplo, a mudança de cidade ou até de país. São considerados dados sensíveis: origem racial ou etnia, opiniões políticas, crenças religiosas, dados genéticos, dados biométricos, adesão sindical, saúde e vida ou orientação sexual. A seguir, esses tipos de dados são apresentados juntamente com seus símbolos e posteriormente com suas definições.

Figura 12 - Dados pessoais sensíveis
Fonte: Próprio autor.

➔ Origem Racial ou Etnia: a origem racial ou etnia pode causar perseguições dependendo do cenário. Muitas guerras foram causadas e ainda são até hoje devido à origem racial ou etnia de uma pessoa.

➔ Opiniões Políticas: a opinião política é considerada um dado sensível, pois ainda existem muitas divergências de opiniões entre as pessoas e também fanatismo político que colocam em risco a vida de muitas pessoas.

➔ Convicção Religiosa: dependendo da situação, essas convicções podem causar discriminações ao titular dos dados.

➔ Dados Genéticos: após o mapeamento do genoma humano, é possível a partir dos dados genéticos realizar o mapeamento da pessoa, identificando seus interesses, cor do cabelo, pele, cor dos olhos entre outras informações. Como os dados genéticos são únicos e não podem ser alterados, são considerados dados sensíveis.

➔ Dados Biométricos: são considerados dados pessoais sensíveis pois não podem ser substituídos e cada pessoa possui apenas 10 dados biométricos. Caso ocorra a violação desses dados, o titular é impossibilitado de utilizá-los.

➔ Filiação Sindical ou organização de caráter religioso, filosófico ou político: a divulgação desse tipo de dado a empresas pode prejudicar um trabalhador, dependendo de sua adesão sindical e da postura da empresa.

➔ Saúde: dados sobre a saúde de uma pessoa podem colocar em risco à vida do titular ou causar uma discriminação dependendo das doenças que a pessoa possui ou já possuiu.

➔ Vida ou orientação sexual: a orientação sexual ou opções de relações sexuais durante a vida de uma pessoa podem causar represálias e preconceito, podendo em alguns casos colocar o titular em risco de vida, uma vez que coloca a vida dele em perigo.

A partir da análise dos tipos de dados pessoais sensíveis descritos acima, é importante a identificação do armazenamento desses dados dentro da organização e a validação da necessidade em mantê-los, principalmente pelos riscos oferecidos ao titular no caso de violação desses dados pessoais. Para o *site* ConectaJá (2020), a utilização dos dados pessoais sensíveis exige uma finalidade específica, obrigando o consentimento do titular a menos que esteja ligado à situações de uma obrigação legal.

3.3 Estrutura da lei

A LGPD está disposta em diversos artigos com uma certa organização, mas que, no geral dificultam a criação de um modelo ou mapa mental. Algumas fontes, como Ramos (2020) afirmam que a lista de críticas à LGPD é extensa, com diversas obrigações ambíguas e um custo alto para fiscalização e aplicação.

Para facilitar a compreensão desse assunto apresentado nesta pesquisa, os artigos da LGPD foram organizados em 4 grandes blocos, que juntos formam uma estrutura que permite cumprir o objetivo principal da lei: garantir a privacidade dos titulares de dados. Esta estrutura é composta pelas "partes envolvidas", pelas "bases legais", pelos "princípios para o tratamento dos dados pessoais" e pelos "direitos do titular". A seguir, a imagem ilustrativa do mapa mental.

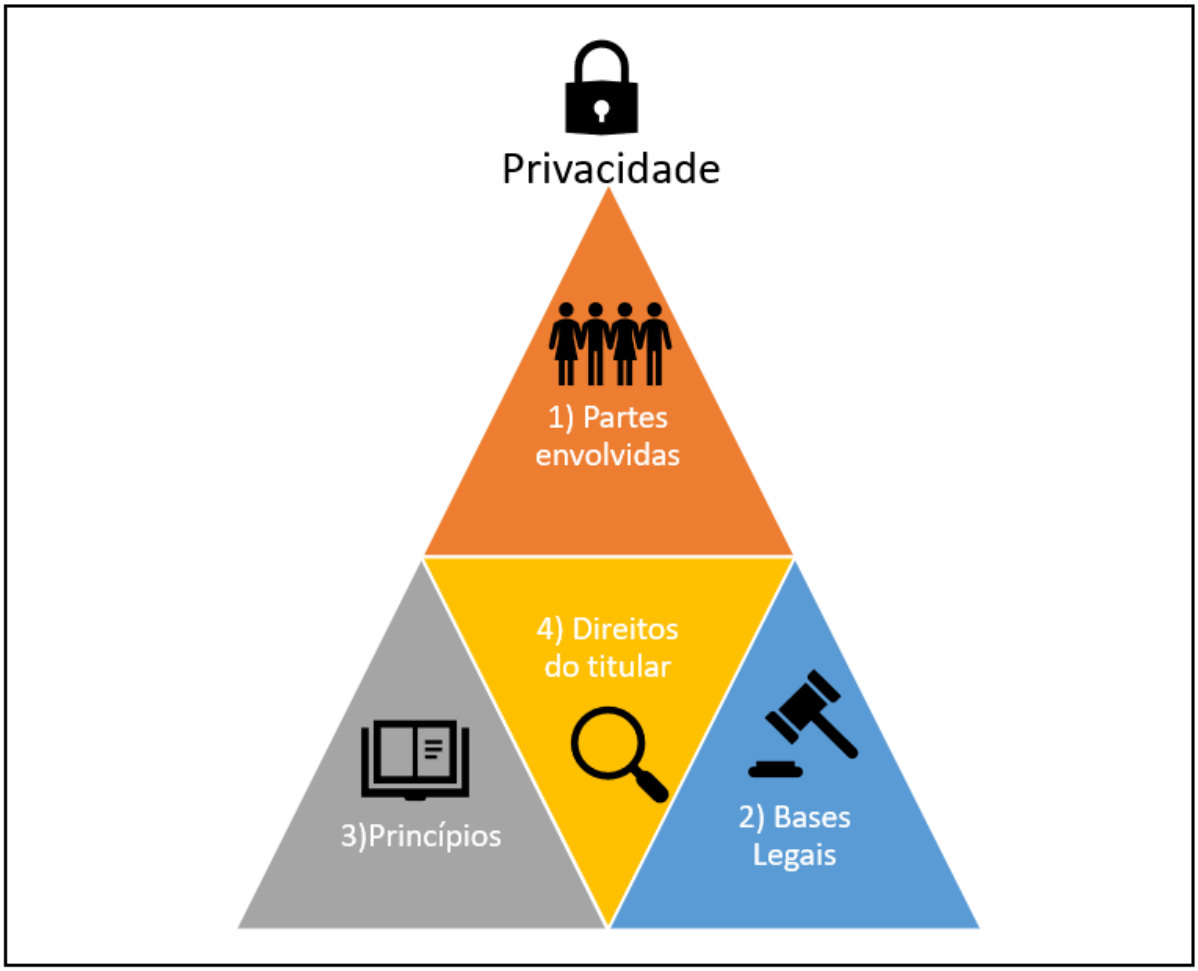


Figura 13 - Estrutura da LGPD
Fonte: Próprio autor.

Dessa forma, para verificar se a lei é atendida deve-se passar pelos 4 grandes grupos, identificando se a organização está agindo de acordo com a lei. Além disso, é importante pensar nos dados como algo vivo, com ciclo de vida, que nasce, cresce e um dia morrerá. Da mesma maneira deve ocorrer com os dados pessoais de um cidadão, pois ele é fornecido, é processado conforme alguma finalidade específica e, após esse processamento, deverá ser excluído de dentro da organização. A seguir, expõem-se separadamente os quatro passos, que possibilitam a construção do triângulo.

O primeiro passo contempla as partes envolvidas, nele descrevem-se os papéis exercidos pelas organizações ou pessoas durante o processo de tratamento de dados pessoais. A lei prevê cinco papéis durante o ciclo de vida de um dado. Cada papel possui uma responsabilidade e uma atuação diferente com o objetivo final de garantir a privacidade do cidadão.

No segundo e terceiro passo, definem-se as estruturas da pirâmide. No segundo passo, encontra-se as dez bases legais para o tratamento dos dados. Partindo dessa premissa, um dado somente pode ser tratado se for garantido que seu tratamento esteja especificado em pelo menos uma das bases legais prevista pela lei. Sem uma base legal, o tratamento não poderá ser realizado, devendo ser apagado ou anonimizado da estrutura da organização.

O lado esquerdo da pirâmide prevê as regras e os objetivos que devem ser cumpridos durante o tratamento de dados, são os chamados princípios para o tratamento de dados. E ao meio, há os direitos que um titular tem em relação aos seus dados pessoais, assim ele poderá exigir do controlador alguns direitos específicos sobre suas informações.

O objetivo principal da lei está no topo da pirâmide, a privacidade. Dessa forma, o tratamento de dados deve garantir que todos os grupos da LGPD visem a privacidade dos dados do titular. A privacidade é o objetivo da LGPD, além de ser direito de um cidadão, conforme previsto Constituição Federal.

Abaixo, é apresentado o detalhamento de cada um dos passos para a construção da estrutura da LGPD.

3.3.1 Partes envolvidas

O primeiro passo na LGPD é identificar as partes envolvidas no processo de proteção dos dados pessoais. Em muitos momentos uma pessoa poderá desenvolver mais de um papel no ciclo de vida dos dados, porém é importante identificar suas principais responsabilidades. Abaixo, seguem informações sobre as partes envolvidas no processo de tratamento de dados pessoais e previstas na LGPD.

3.3.1.1 Titular dos dados

Pessoa física que fornece seus dados pessoais ao consumir algum produto ou serviço. De forma resumida, considera-se titular dos dados, os “clientes” de uma organização, a qual mantém um relacionamento comercial com o controlador por algum fim específico.

3.3.1.2 Controlador

Pessoa jurídica ou física que recebe os dados pessoais de um titular para executar algum tratamento desses dados. Seu principal papel é tomar as decisões relativas ao tratamento dos dados pessoais de seus titulares e proteger a privacidade das pessoas físicas que lhe confiaram os seus dados.

3.3.1.3 Operador

Pessoa física ou jurídica contratada pelo controlador para operar os dados dos titulares. O operador realiza os tratamentos de dados a serviço do controlador, definidas por este, a forma de utilização.

3.3.1.4 Encarregado (DPO)

Contratado pelo controlador, tem como principal função intermediar a comunicação entre as demais partes. O DPO é o representante dos titulares para os controladores. Além da função de intermediar as comunicações, o DPO auxiliará os controladores de dados e os operadores, direcionando-os na melhor forma para o tratamento dos dados. Além disso, ele pode realizar auditorias para garantir a qualidade dos processos necessários para atender a LGPD.

A LGPD obriga ao DPO que forneça de forma clara e transparente seus dados e contatos para que qualquer titular de dados tenha acesso a essas informações e possa entrar em contato quando necessário. É recomendável que esses dados estejam disponíveis no *site* da empresa.

3.3.1.5 Autoridade Nacional de Processamento de dados (ANPD)

Órgão do Governo responsável por fiscalizar a conformidade com a LGPD por parte das demais partes envolvidas. Ele será responsável pela aplicação de multas e pela realização de auditorias, verificando a aderência da LGPD dentro das organizações. Para alguns especialistas, muitos pontos ainda obscuros descritos na lei, serão resolvidos após a criação e estruturação da ANPD. Mesmo com a vigência da lei, a autoridade nacional encontra-se em estruturação.

Conforme C3dweb (20--), a ANPD já teve sua estrutura aprovada, contendo o quadro dos funcionários e regras para funcionamento.

Abaixo, os papéis definidos pela LGPD:

Figura 14 - Partes envolvidas
Fonte: Próprio autor.

3.3.2 Bases legais para tratamento de dados pessoais

Para que seja possível realizar qualquer tipo de tratamento de dados pessoais, o controlador precisa ter um motivo legítimo, ou seja, uma boa razão para esse tratamento de dados. Esse motivo legitimo é considerado pela lei como uma Base Legal para tratamento de dados pessoais. As bases legais que a LGPD estabelece estão apresentadas a seguir.

Figura 15 - Bases legais
Fonte: Próprio autor.

3.3.2.1 Cumprimento de obrigação legal a que o controlador está sujeito

Sob esta base legal o controlador trata os dados para cumprir qualquer obrigação legal à qual ele esteja sujeito. Dessa forma, esta base legal permite que a LGPD não entre em conflito com outras leis existente no país, o que geraria um grande conflito de interesses e aberturas para que o titular dos dados gere reclamações por não concordar com tratamento dos dados pessoais em determinações legais.

Esta base garante que os dados sejam tratados apenas enquanto a obrigação legal for necessária, a partir do momento que não existir motivos para tratamento das obrigações legais, os dados precisarão ser excluídos ou se faz necessário o enquadramento em outra base legal, como o consentimento do titular de dados.

3.3.2.2 Execução de um contrato no qual o titular é parte

Sob esta base legal o controlador dos dados trata os dados pessoais para executar um contrato no qual o titular dos dados é parte deste contrato. Nesta base, o titular dos dados autoriza o tratamento de seus dados ao adquirir um produto ou serviço. Esta base legal se assemelha com a base número 10 – consentimento do titular, porém, caso haja a execução de um contrato, o consentimento não poderá ser revogado pelo titular dos dados, pois se faz necessário o tratamento para execução do contrato pré-estabelecido. Ao finalizar a execução

do contrato, o controlador não pode mais efetuar o tratamento dos dados sem que exista uma nova base legal para o fim.

3.3.2.3 Proteger o interesse vital da pessoa em causa ou de outra pessoa física

Esta base legal se aplica com o intuito de proteger a vida ou a qualidade de vida do titular de dados ou de outra pessoa física. Quando houver a necessidade de proteger a vida de uma pessoa, seus dados podem ser tratados de acordo com esta base legal, sem a necessidade prévia do consentimento do titular.

Para Gualtieri (2019), esta base legal é específica e pode realizar o tratamento inclusive em dados sensíveis se forem indispensáveis para a proteção da vida do titular dos dados.

3.3.2.4 Para a tutela da saúde

Esta base legal é utilizada para a tutela da saúde dos titulares de dados, sendo necessária aos profissionais de saúde. Nesta base legal, é possível realizar o tratamento de dados sensíveis, mesmo sem a autorização do titular dos dados, se o motivo for identificável como tratamento para garantir a saúde da pessoa. A base legal para a tutela da saúde se assemelha com a base de interesse vital da pessoa.

De acordo com Gualtieri (2019), esta base legal possui uma especificidade no artigo 11 da lei, em que é possível o compartilhamento e a comunicação entre controladores no caso da prestação de serviço de saúde.

3.3.2.5 Interesse público ou no exercício da autoridade oficial

Para esta base, os órgãos da administração pública no exercício da autoridade oficial poderão tratar os dados pessoais, porém os mesmos são obrigados a utilizarem a transparência no tratamento desses dados pessoais, a menos que eles sejam utilizados para fins de segurança pública, defesa nacional ou outras atividades necessárias no processo de investigação nas quais o titular dos dados seja sujeito.

3.3.2.6 Realização de estudos por órgão de pesquisa

Esta base legal permite que estudos sejam realizados por órgãos de pesquisa com dados pessoais, porém ressalta que sempre que possível os dados sejam anonimizados (item 4.2), garantindo a privacidade dos titulares de dados. Dessa forma, caso os dados pessoais não

sejam necessários para a realização dos estudos, os mesmos devem ser descaracterizados utilizando apenas os conceitos gerais desses dados.

3.3.2.7 Exercício de direitos em processo judicial, administrativo ou arbitral

Esta base legal permite a utilização dos dados em processos judiciais, administrativos ou arbitrais. Esta base garante a criação de provas para os processos existentes, possibilitando o direito de defesa de um cidadão através de informações pessoais.

3.3.2.8 Proteção de crédito

Esta base foi criada para evitar que usem uma brecha existente na LGPD em relação à proteção de crédito, que permitiria que as pessoas físicas não fossem cobradas por dívidas existentes. Dessa forma, mesmo sem o consentimento do titular, se houver qualquer tipo de dívida, o titular dos dados terá seus dados tratados para fins de cobranças e negociações.

Conforme Gualtieri (2019), muitos debates foram suscitados no meio acadêmico a respeito da inclusão de dados no Cadastro Positivo. Ele afirma que esses conflitos só poderão ser superados com a criação da ANPD, que realizará determinações sobre o assunto.

3.3.2.9 Interesses legítimos do responsável pelo tratamento

A base legal de legítimo interesse é considerada por muitos uma base frágil em sua utilização, por permitir vários entendimentos sobre o assunto. A base legal de legítimo interesse deve ser muito bem estudada antes de sua utilização, pois poderá acarretar problemas futuros. Na dúvida se está base pode ser aplicada, a obtenção do consentimento do titular é a melhor opção.

Gualtieri (2019) afirma que essa é uma base problemática, recomendada apenas quando não houver outra base legal aplicável para o tratamento dos dados pessoais. Para Soares (2019) a base legal do legítimo interesse é clara e está relacionada ao interesse do controlador ou de terceiros que deve ser tutelado.

3.3.2.10 Consentimento do titular

A base legal do consentimento do titular, garante ao controlador que o titular dos dados aprovou o tratamento de seus dados para algum fim específico e pré-determinado. Esse consentimento deverá ser descrito ao titular dos dados de forma clara e transparente para que não existam dúvidas por parte do titular.

Antes da utilização da base legal consentimento, o controlador deve primeiramente analisar se é possível aplicar uma das oito bases legais descritas anteriormente. Isto porque obter o consentimento pode ser custoso e nem sempre será possível, além de ser uma base legal frágil, em que o titular dos dados poderá, a qualquer momento, revogar esse consentimento.

Caso não seja possível, deverá averiguar se o tratamento que precisa realizar pode utilizar a base legal de legítimo interesse do controlador. Por exemplo, quando uma empresa precisa monitorar os *e-mails* e a navegação de internet de seus funcionários para garantir a segurança da sua rede e também para evitar o vazamento de informações secretas. Sendo este um interesse legítimo da empresa, bem fundamentado e justificável, não seria necessário obter o consentimento dos funcionários, apenas informá-los, seguindo os princípios da LGPD.

3.3.3 Princípios das partes envolvidas

A lei prevê seis regras ou valores que precisam ser cumpridos durante o tratamento dos dados pessoais, além das conformidades com as bases legais. Essas regras ou valores são os princípios considerados em lei que o controlador deve seguir durante todo o tratamento de dados pessoais. Esses princípios podem ser observados na figura a seguir.

Figura 16 - Princípios definidos por lei
Fonte: Próprio autor.

3.3.3.1 Finalidade

Os dados pessoais devem ser coletados para fins específicos, explícitos e legítimos. A comunicação da finalidade deve ser declarada antes do início do processamento e caso exista mais de uma finalidade para o tratamento dos dados pessoais, todas elas devem ser declaradas ao titular dos dados de forma transparente e que não gere dúvidas em seu tratamento.

3.3.3.2 Necessidade

Os dados pessoais devem ser adequados, relevantes e limitados ao necessário, ou seja, minimizados em sua coleta. Não devem ser mantidos ou retidos por tempo maior que o necessário para atingir os objetivos acordados com o titular.

3.3.3.3 Adequação

Neste princípio, deve ser compatível a finalidade em que o controlador informou ao titular de dados com o tratamento realizado pelo mesmo. A lei deixa explícito que é necessário um cuidado especial com a adequação dos dados sensíveis e que os mesmos estejam sempre atualizados e condizentes com a realidade.

3.3.3.4 Qualidade dos dados

O princípio da qualidade de dados prevê precisão nos dados pessoais e devem ser atualizados, sempre que for necessário. A atualização dos dados deve ocorrer de maneira segura, garantindo que somente seja alterado dados desatualizados.

3.3.3.5 Transparência

Esse princípio prevê que todas as informações passadas pela empresa ao titular de dados, independente do meio de comunicação, devem ser claras, precisas e verdadeiras, aplicando assim o princípio da transparência.

3.3.3.6 Livre Acesso

O titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa ou organização detenha a seu respeito. Essa consulta pode ser realizada através de um sistema, ou abertura de um protocolo, porém de forma simples e clara, não gerando custos extras ao titular dos dados.

3.3.3.7 Segurança

Este princípio prevê que seja utilizada medidas técnicas ou administrativas, visando a proteção dos dados pessoais de acessos sem a devida autorização. Além disso, esse princípio prevê medidas para mitigação de situações de risco que envolvem os dados pessoais que são armazenados. Essas medidas estão relacionadas a procedimentos internos realizados pela área de tecnologia, como o uso de antivírus, o bloqueio de acesso a computadores após período de inatividade entre outros.

3.3.3.8 Prevenção

Neste princípio, é necessário que as empresas adotem medidas prévias para evitar a violação de dados, durante todo o tratamento de dados pessoais. Essas medidas contemplam a gestão de risco e o tratamento das vulnerabilidades existentes dentro da organização. A palavra prevenção garante o sucesso na aplicação da LGPD dentro das organizações, visto que inclusive as sanções são medidas com base na proatividade da mitigação dos riscos.

3.3.3.9 Não discriminação

A LGPD estipula a não realização de tratamento de dados que possuam finalidade abusiva, garantindo a não discriminação dos titulares de dados. Qualquer dos tipos citados não são aceitáveis e fogem desse princípio estabelecido por lei.

3.3.3.10 Responsabilização e prestação de contas

Nestes princípios, verifica-se a demonstração, pelo responsável pelo tratamento (controlador ou operador), da aplicação de medidas eficazes, com o objetivo de aderir as disposições descritas na lei, em relação à proteção de dados pessoais.

3.3.4 Direitos do titular

Além dos princípios que precisam ser seguidos, conforme descrito na LGPD, o titular de dados tem oito direitos estabelecidos por lei. Esses direitos podem ser solicitados pelo titular de dados, ao controlador de seus dados, e o mesmo deverá fornecer ao titular as informações solicitadas de forma rápida, aplicando todos os esforções necessários para atendimento dos direitos do titular de dados.

O período de tempo para que haja esse retorno não é estabelecido em lei, porém é importante ressaltar que as empresas não devem se alongar no retorno das solicitações, pois a LGPD é passível de multa e os direitos estão previstos em lei.

Para Peixoto (2020), a LGPD prevê aos titulares de dados proteção integral a liberdade, privacidade e segurança, sendo protegidas as informações que permitem a identificação de uma pessoa.

Abaixo, estão descritos os oito direitos dos titulares.

Figura 17 - Direitos do titular
Fonte: Próprio autor.

3.3.4.1 Acesso

O titular terá o direito de obter a confirmação do controlador sobre a existência de processamento de seus dados e, em caso positivo, o acesso aos dados juntamente com as informações armazenadas pela empresa ou organização. A seguir, apresenta-se a lista das informações que são parte do direito do titular de dados:

✓ Finalidade: para qual finalidade os dados do titular estão sendo processados. Neste caso, será necessário informar todos os tipos de processamentos existentes e realizados com os dados pessoais do titular.

✓ Categorias: em quais categorias os dados do titular estão classificados. Nesse caso, é possível encontrar a existência de categorias feitas pelo controlador, por exemplo, considerando a classe social em que o titular está enquadrado: classe alta, classe média ou classe baixa. Assim, quando demandado pelo titular, o controlador precisará informar em quais dessas categorias o titular dos dados está classificado e como houve essa classificação.

✓ Destinatários: para quais destinatários o controlador dos dados enviou os dados do titular solicitante. Neste direito do titular, para que seja informado os destinatários, é necessário que o controlador tenha enviado os dados para outras empresas, ou seja, para operadores realizarem o tratamento dos dados pessoais do titular. O atendimento dessa solicitação, necessita de uma rastreabilidade dos compartilhamentos de informações feito pelo controlador.

✓ Período previsto: estabelece qual o período previsto de armazenamento dos dados pessoais do titular. O controlador precisará informar ao titular sobre o tempo que ele irá

reter essas informações em sua estrutura, inclusive o motivo legal da retenção da informação pelo tempo informado.

- ✓ Existência de direitos específicos: caso exista algum direito específico sobre a área de atuação do controlador dos dados, será necessário que o mesmo possua esse conhecimento para informação ao titular dos dados. Um exemplo seria o código do consumidor ou leis municipais.
- ✓ Procedimento de reclamações: será necessário definir um procedimento para que o titular possa, de forma simples e rápida, registrar uma reclamação. Caso o titular dos dados entre em contato com o controlador, será necessário que esse procedimento seja repassado ao titular.
- ✓ Fontes indiretas de coleta: neste direito, o titular poderá solicitar a informação para conhecer se houve a captação dos seus dados por outra fonte. Portanto, é importante que o controlador saiba de onde obteve cada um dos dados do titular, pois talvez seja necessário repassar esse tipo de informação.
- ✓ Existência de tomada de decisão automática: caso exista algum processo automatizado, no qual as máquinas tomam decisões em algum momento do processo de tratamento de dados, o titular terá o direito de saber, além da existência desse processo, a respeito de como são realizadas as tomadas de decisões automatizadas.

3.3.4.2 Correção de dados incompletos

O titular tem o direito de retificar seus dados a qualquer momento de forma rápida e sem dificuldades. Porém, para que o processo de retificação ocorra de forma adequada, conforme indicado pela LGPD, é importante que exista um processo para atualização desses dados cadastrais garantindo a qualidade desses dados.

Não são todos os dados que poderão ser atualizados, apenas dados que estejam inconsistentes ou incorretos podem ser retificados. Para garantir que apenas esses dados sejam atualizados, o controlador precisará definir meios de atualização verificando assim a integridade e a qualidade dos dados pessoais.

Dessa forma, se faz necessário que o controlador informe aos operadores, com os quais tenha realizado o compartilhado desses dados, para que ele realize a retificação dos dados do titular. Portanto, no caso de retificação, é necessário que os mesmos sejam atualizados em todos os compartilhamentos de dados.

3.3.4.3 Esquecimento

O titular tem o direito de solicitar à exclusão de seus dados armazenados por um controlador ou operador.

Este direito pode ser exercido contra os controladores, os quais devem responder com a confirmação sem atrasos indevidos conforme previsto em lei. Para realizar tal confirmação, os controladores têm o prazo máximo de 1 mês, a contar da data da solicitação. Entretanto, o titular dos dados, só poderá realizar a solicitação de exclusão, quando houver um dos motivos abaixo listados:

- ✓ Dados não são mais necessários para os fins, ou seja, quando os dados armazenados não são necessários para o fim inicialmente proposto, ou que o fim já tenha sido alcançado.
- ✓ Retirada de consentimento, ou seja, quando houve o consentimento dado pelo titular dos dados, porém o mesmo não quer mais que esse consentimento continue. Caso tenha ocorrido mais de um consentimento, o titular de dados poderá retirar um, mais de um ou todos os consentimentos concedidos ao controlador dos dados.
- ✓ Quando houver ofertas de serviços e o titular dos dados for menor que 18 anos, o mesmo, ou seu responsável legal, poderá solicitar seu esquecimento.
- ✓ Quando houver objeções ao processamento que está sendo efetuado com os seus dados pessoais, havendo a possibilidade do titular dos dados solicitar o seu esquecimento.
- ✓ Quando o controlador ou operador estiverem realizando um processamento ilegal com os dados do titular, o mesmo poderá solicitar que seja esquecido toda e qualquer informação contida dentro da organização. Também neste caso, o controlador deverá informar aos operadores, com os quais tenha realizado o compartilhamento desses dados, para que repitam o mesmo procedimento de esquecimento dos dados pessoais do titular.

3.3.4.4 Revisão de decisões automatizadas

O titular tem o direito de solicitar que as decisões automatizadas realizadas com seus dados pessoais sejam revisadas, ou seja, qualquer tipo de processamento que seja realizado por uma máquina e não passe pela análise de uma pessoa é passível desse direito.

Nesse caso, caso o controlador de dados não concorde com a decisão automatizada, é possível que o titular dos dados solicite ao controlador que revise as decisões tomadas por uma máquina, sendo necessária a intervenção humana.

3.3.4.5 Notificação

O titular tem o direito de ser notificado sobre as operações relevantes que serão executadas com seus dados pessoais, incluindo as requisições que tenha feito com relação aos demais direitos. Dessa forma, todo e qualquer tratamento de dados realizado deverá ser comunicado via *e-mail*, SMS, ligação ao titular dos dados ou de outra forma possível para que seja efetivada a notificação.

3.3.4.6 Portabilidade

O titular tem o direito de transmitir seus dados para outro controlador, ou seja, para um concorrente do controlador. A portabilidade já é um direito existente nas telefonias móveis, onde é possível trocar de operadora com as mesmas informações de telefone já utilizadas. Após a vigência da lei, esse direito se estendeu para qualquer fim comercial.

É importante ressaltar que esse direito não se aplica quando o processamento é para interesse público ou no exercício da autoridade oficial.

Em linhas gerias, o titular tem o direito de receber seus dados pessoais em formato:

- ✓ Estruturado;
- ✓ Comumente utilizado;
- ✓ Passível de leitura por máquina.

As definições acima ainda não estão bem declaradas e definidas, aguardando assim, a criação e estruturação da ANPD para que seja possível uma organização e padronização da estrutura de portabilidade dos dados pessoais.

3.3.4.7 Revogação do consentimento

O titular poderá revogar o consentimento a qualquer tempo, mediante sua manifestação expressa, através de um procedimento disponibilizado pelo controlador de dados, sendo de forma rápida e simples.

Além disso, o titular poderá se opor ao tratamento de seus dados, dispensando o consentimento, quando a finalidade informada pelo o controlador não for transparente.

Nesse caso, também é necessário que o controlador informe de maneira imediata aos operadores, com os quais tenha realizado o compartilhado desses dados, para que repitam o mesmo procedimento, revogando assim o consentimento do titular.

3.3.4.8 Cumprimento das obrigações legais

O titular tem o direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, como os princípios e bases legais, mesmo para os casos de dispensa de exigência de consentimento.

Além disso, a lei estabelece a inversão do ônus da prova, por isso é o acusado que deve provar sua inocência. Conforme *site* Direitonet (2016, np.), o ônus da prova "é o encargo do sujeito para demonstração de determinadas alegações de fato.".

Com a inversão do ônus da prova prevista pela LGPD, as alegações não precisam ser provadas e sim a sua defesa. Por exemplo, caso o titular denuncie o controlador por algum tratamento inadequado de seus dados, é o controlador que deverá provar que agiu de acordo com a lei, utilizando de todos as medidas necessárias para garantir a privacidade do titular dos dados. Isso porque a legislação brasileira segue os princípios do direito Europeu que prevê, ao lado mais fraco, vantagens em sua defesa. Para Gonçalves (2013), a inversão do ônus da prova em favor ao consumidor facilita sua defesa no processo.

3.4 Como uma empresa deve agir com relação à violação de dados pessoais?

Trata-se de um ponto delicado envolvendo principalmente a ética das pessoas envolvidas em uma violação de dados pessoais. Para que a empresa aja de forma correta com a lei e todo o processo seja realizado, faz-se necessário uma mudança na cultura presente dentro das organizações, tornando a privacidade como padrão em qualquer processo de tratamento de dados e não uma parte do tratamento, pois assim facilitaria a tomada de medidas após a violação dos dados pessoais. Conforme reportagem de Tiegh (2020), a construtora MBigucci enfrentou desafios ao rever os processos e as informações que eram coletadas e não úteis para a construtora. Um exemplo citado na reportagem é o pedido aos clientes, em plantões de venda, sobre o time que o interessado torce, utilizando essa informação posteriormente para sorteios e promoções.

Para a LGPD, assim que houver a identificação de violação dos dados pessoais, a pessoa que o identificou deve informar imediatamente o DPO/Encarregado do controlador. Geralmente, a pessoa que identifica essa violação está envolvida nesse processo e tem receito de comunicar, porém é importante que essa ação seja realizada de forma rápida e precisa para evitar mais danos futuros. Com essa informação, o DPO tem a obrigação de comunicar o mais rápido possível a ANPD, além de tomar outras medidas necessárias para mitigação das consequências causadas a partir da violação dos dados pessoais. Além da comunicação à

ANPD, o DPO ou o encarregado do controlador devem comunicar o titular dos dados quando houver situações em que:

- os dados forem sensíveis;
- os dados não estavam criptografados;
- não foram tomadas medidas de mitigação dos impactos;
- não houve mitigação dos impactos;
- o esforço de comunicar individualmente a cada titular não for desproporcional.

Caso um dos fatores acima seja negativo, o controlador não é obrigado a comunicar aos titulares de dados de que houve a violação dos seus dados, bem como os impactos que foram causados com essa violação.

Abaixo, segue imagem com o processo de violação dos dados pessoais.

Figura 18 - Processo após violação dos dados
Fonte: Próprio autor.

3.5 Como uma pessoa deve agir no caso de violação dos seus dados pessoais?

O titular dos dados que se sentir lesado tem algumas alternativas a seguir, mesmo antes da criação da ANPD. Segundo Tiegh (2020), mesmo sem a ANPD, um dos artigos da LGPD possibilitam que o titular faça uma denúncia aos órgãos de defesa do consumidor ou

gere um processo judicial, como o caso já conhecido e publicado em jornais eletrônicos como G1 (2020) em que a Cyrela foi a primeira empesa sob pena de multa de R$300,00 por contato indevido e ao pagamento de R$10.000,00 reais por danos morais, sob a infração da LGPD. Na reportagem, o G1 explica que a Justiça de São Paulo determinou a multa após o cliente ter recebido ligações não autorizadas de instituições financeiras, consórcios e empresas de arquitetura e mobiliário planejado.

A ANPD, após sua criação, receberá as denúncias de pessoas naturais que se sentirem prejudicadas pelo vazamento de seus dados pessoais. Porém, muitos especialistas discutem que nem todas as denúncias serão analisadas pela Autoridade nacional, alguns estudiosos no assunto apontam que somente vazamentos com grandes impactos serão analisados pela ANPD. Conforme o *site* de Serviço Federal de Processamento de Dados, Serpro (20--), a ANPD atuará como um órgão a serviço do cidadão.

Além da ANPD, o titular dos dados poderá entrar em contato com o controlador de seus dados e solicitar seus direitos, como o de esquecimento, conforme indicados anteriormente.

Todas as organizações com fins lucrativos, que tratam dados pessoais, deverão disponibilizar de fácil acesso um canal de atendimento para reclamações e o contato do DPO responsável, para que assim seja possível, além da garantia do direito à privacidade, que o titular tenha acesso facilitado às empresas que detém suas informações pessoais.

Segue abaixo imagem de como o titular de dados poderá proceder no caso de uma possível violação de seus dados pessoais.

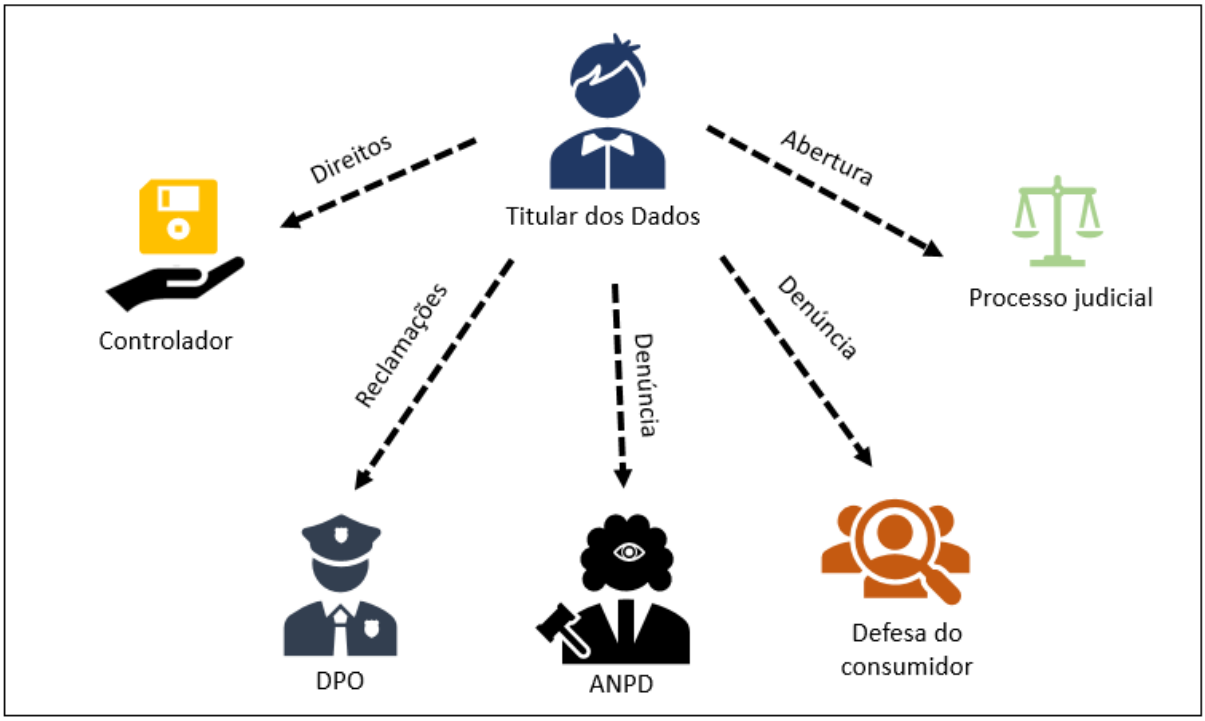


Figura 19 - Como o titular poderá proceder
Fonte: Próprio autor.

CAPÍTULO 4: QUAL IMPACTO E ABRANGÊNCIA DA LGPD?

Neste capítulo será exposto os impactos causados nas organizações a partir da entrada em vigor da LGPD, bem como suas penalizações e a medição realizada para a definição das penalizações. Além disso, o capítulo contará com as boas práticas para adequação à LGPD e um breve resumo sobre as leis de proteção de dados em países considerados referência no assunto.

4.1 Impacto da LGPD

A LGPD forçou as empresas a pensarem novas estratégias em seus negócios, para adaptação e aplicação das novas regras impostas pela lei. A privacidade dos dados, antes em segundo plano para as organizações, passou a ser vista como prioridade essencial e tem somado muitos esforços nos últimos tempos. Conforme Peixoto (2020), a LGPD terá o impacto mais significativo que uma legislação nacional já alcançou. A autora ressalta no texto que este impacto existe devido a milhões de empresas brasileiras trabalharem de alguma forma com dados pessoais de clientes. Considerando que a lei mudou as normas de proteção de dados, as quais deixa de ser uma opção e se torna uma obrigação legal, as mudanças nas organizações serão relevantes. O texto de Peixoto (2020), foi publicado em Janeiro de 2020, no entanto, um ano depois dessa publicação, os impactos ainda são visíveis no meio corporativo. Praticamente todas as empresas falam a todo tempo sobre a LGPD. É possível considerar que o principal impacto da LGPD tenha sido a mudança de paradigma trazendo a proatividade e a conscientização das organizações como ferramenta para combater as penalizações. Conforme informado no *site* Incontract (20--), é importante que haja uma mudança dentro das organizações, de modo que comecem a respeitar os dados de clientes, fornecedores e parceiros. Dessa forma, será necessária a criação de meios para, não apenas garantir a proteção de dados, mas também criar uma relação de confiança com os parceiros e clientes.

O *site* Serpro (20—, np.) disponibiliza uma lista com os ramos mais impactados pela LGPD, são eles: “Software e tecnologia - Direito e advocacia - Financeira e seguros - Comércio digital - Pesquisa e perfilamento - Saúde privada e planos - Publicidade e marketing”. Além disso, o *site* ressalta que a Lei tem equilíbrio nas esferas federal estadual e municipal, o que diminui a concorrência desleal e os obstáculos ao desenvolvimento econômico do país.

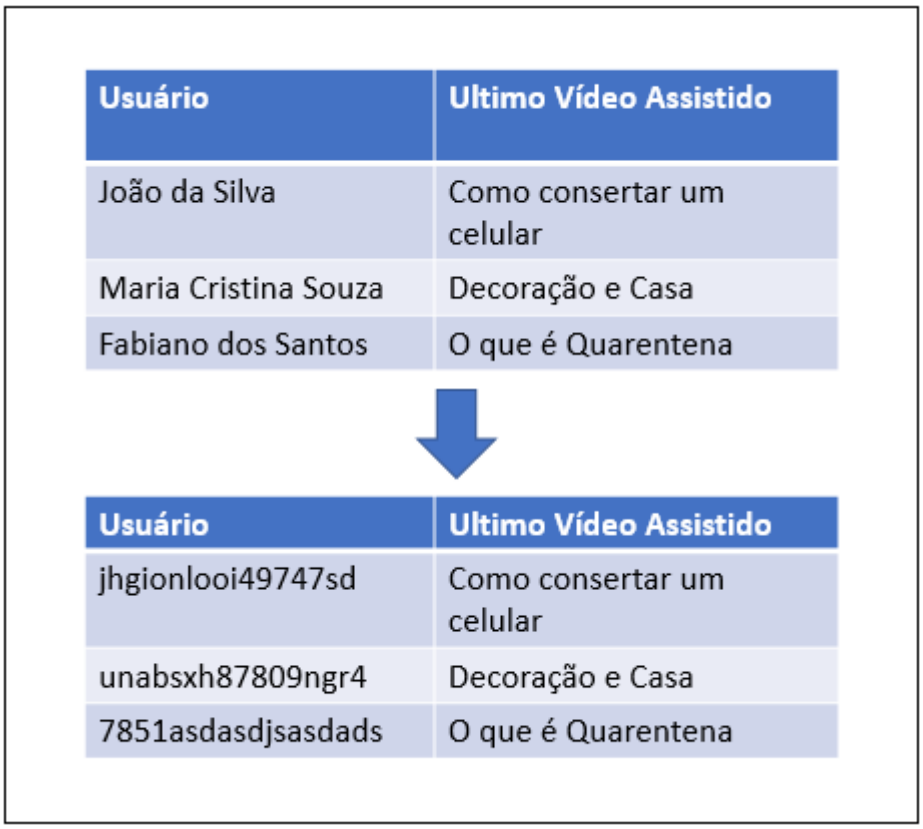
Algumas práticas existentes no mercado como a proteção *By Design*, que surgiu em meados da década de 90, foi utilizada por várias organizações, para simplificar a implantação da LGPD. Em termos gerais, a técnica de proteção *By Design*, criada pela área de Engenharia de Sistemas, pensa na privacidade do usuário em todo o processo ou projeto dentro da organização, ou seja, a privacidade é definida como padrão desde o início da proteção de dados, trazendo a ideia principal da criação de uma cultura corporativa. Para o dicionário on-line Dicio (2021) a palavra **cultura** significa conjunto de hábitos, normas ou crenças. Concluindo assim que, com a implantação da prática de proteção *By Design*, existirá a criação de uma cultura corporativa na qual os colaboradores terão o hábito da privacidade integrado à tecnologia ou aos processos existentes dentro da empresa.

4.2 Anonimização de dados

O processo de anonimização dos dados está relacionado com a descaracterização de alguns dados contidos dentro da base de dados Digital. Este processo é considerado unilateral, ou seja, não é reversível. A partir do momento que os dados são anonimizados, eles passam a não ser mais dados pessoais e não são aplicáveis à LGPD, conforme descrito na própria lei. Dessa forma, o processo de anonimização dos dados pode ser aplicado quando não existe mais bases legais para o tratamento dos mesmos, porém existe a necessidade de mantê-los para utilização no futuro, por exemplo no caso de estatísticas e análises gerenciais.

Em um artigo publicado na Nature Communication, Rocher *et al.* (2019) identificaram 99,98% dos dados anonimizados, através de conjuntos de características identificáveis. Com isso, foi explorado como inadequada as técnicas atuais de anonimização dos dados.

Abaixo, expõe-se um exemplo meramente ilustrativo de como os dados ficariam após o processo de anonimização.



Usuário	Ultimo Vídeo Assistido
João da Silva	Como consertar um celular
Maria Cristina Souza	Decoração e Casa
Fabiano dos Santos	O que é Quarentena

Usuário	Ultimo Vídeo Assistido
jhgionlooi49747sd	Como consertar um celular
unabsxh87809ngr4	Decoração e Casa
7851asdasdjsasdads	O que é Quarentena

Figura 20 - Dados anonimizados
Fonte: Próprio autor.

4.3 Boas práticas e governança

Conforme Brasil (2018), a Lei geral de proteção de dados, em seu Artigo 50, prevê que o controlador e o operador podem formular regras de boas práticas e governança a fim de possibilitar a organização e o bom funcionamento dos procedimentos internos, garantindo a proteção dos dados pessoais. A lei prevê que a implementação do programa de governança da privacidade, possua no mínimo:

a) O comprometimento e a adoção de processos e políticas, com a finalidade de realizar práticas relacionadas à proteção de dados pessoais;

b) A aplicabilidade a todos os dados pessoais controlados, independentemente do modo de coleta;

c) A adaptação a toda estrutura, volume e dados sensíveis;

d) O levantamento dos impactos e riscos estabelecendo mitigação a cada um deles;

e) Uma relação transparente com o titular dos dados, assegurando a participação do mesmo em todos os processos de tratamento de dados.

f) A integração com o processo de governança geral da empresa aplicando supervisão interna e externa;

g) Uma resposta rápida em casos de incidentes;

h) Revisão e atualização, a partir de avaliações contínuas no processo.

O programa de governança é uma saída proposta por lei para que o controlador fique aderente a nova lei de proteção de dados. Para tanto, existe a possibilidade da ANPD solicitar que o controlador demonstre, no momento oportuno, que seu programa de governança é efetivo. Dessa forma, o programa de governança deve estar vivo dentro da organização, com procedimentos de melhoria contínua, para que realmente as boas práticas sejam aplicadas, criando condições à organização de atender as obrigações previstas em lei. Além disso, a LGPD ressalta que essas boas práticas e governança precisam ser atualizadas constantemente e que a ANPD encorajará a adoção dessas práticas na empresa.

4.4 Compliance

Compliance vem do verbo em inglês *To comply* que significa obedecer, concordar e consentir para cumprimento. Dessa forma, entende-se como *compliance* uma política ou um conjunto de regras adotadas por uma organização. Para tanto, as empresas adotam um programa de *compliance* para definições de políticas com o objetivo de se adequar às legislações vigentes. Siteware (2017) afirma que *Compliance* está relacionada à conduta e à adequação da empresa com as leis e regulamentos em vigor. Já para Donella (2019), o termo está associado à integridade corporativa, o que significa estar alinhado com as regras corporativas, cumprindo-as de forma correta. O *Compliance* surgiu no Brasil após a criação da Lei 2.846 conhecida como lei anticorrupção. Essa lei surgiu para evitar que empresas se beneficiem de propinas em troca da realização de um determinado trabalho. Empresas que oferecem serviços, principalmente para os setores públicos, precisaram se adequar e definir regras internas evitando ocorrências de vantagens obtidas ou pretendidas.

Donella (2019) afirma que não pensar em programas de *compliance* atualmente nas companhias pode gerar vários riscos, inclusive pode levar a organização sofrer sanções administrativas, perda financeira e perda da reputação. Com o passar do tempo, os programas de *Compliance* tornaram-se cada vez mais solicitados dentre as organizações e seu uso tem crescido muito devido à aplicabilidade da LGPD. Atualmente, as frentes de trabalho do *Compliance* são:

> (...) prevenção à lavagem de dinheiro e financiamento ao terrorismo (PLD-FT), anticorrupção, fraude, privacidade, monitoramentos, Código de Conduta, Código de Ética, integridade, treinamentos, avaliação de riscos internos, reportar os erros, atendimento imediato, canais de denúncia. (DONELLA, 2019, np).

De acordo com a equipe Direito Profissional do *site* Ambra University (2019), o *Compliance* se relaciona com a LGPD, pois a Figura do DPO deve ser de um profissional que tem conhecimento também em *Compliance*, governança e risco a fim de garantir a aplicabilidade correta da lei. As figuras do DPO e do *Compliance Officer* se sobrepõem neste novo cenário com desafios impostos pela nova LGPD.

Para Oliveira *et al.* (2019), uma organização se mantem em *compliance* com a nova LGPD, quando, além de considerar tudo que é exigido pela lei, ela também elabora adequadamente um termo de uso e uma política de privacidade que seja transparente ao titular dos dados.

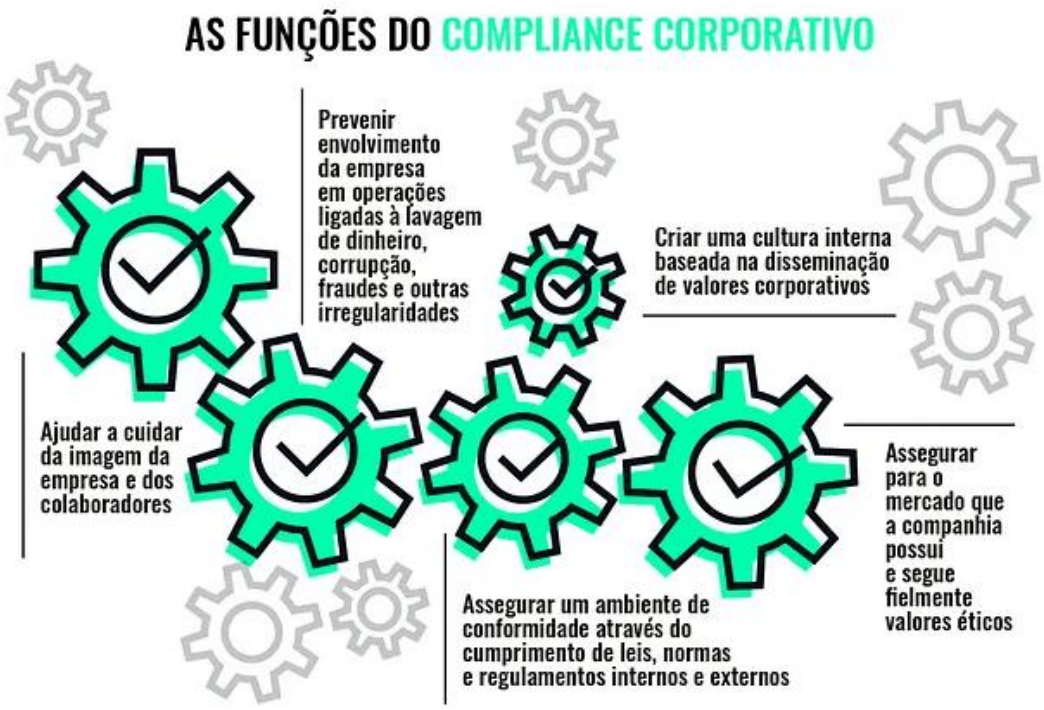


Figura 21 - As funções do *Compliance* corporativo
Fonte: Donella (2019, np).

4.5 Penalizações

Mesmo com a entrada da LGPD em vigor a partir e setembro de 2020, as penalizações ou multas só poderão ser aplicadas pela ANPD a partir de agosto de 2021, porém, como já mencionado, atualmente já foram aplicadas sanções relacionadas a LGPD. A lei prevê nove tipos de penalizações para as pessoas naturais ou jurídicas que não estiverem de acordo com

os artigos descritos na legislação. Em caso de violação de dados pessoais, a ANPD poderá impor ao controlador e ao operador algumas formas de penalização, as quais estão expostas a seguir.

4.5.1 Eliminação dos dados pessoais

Nesta forma de penalização, o controlador deve eliminar todos os dados pessoais dos titulares afetados com a violação, contidos em sua estrutura. Essa eliminação ocorre apenas aos dados pessoais aos quais se referem a infração.

4.5.2 Bloqueio do tratamento dos dados para qualquer titular

Nesta sanção administrativa, o controlador e os operadores serão impedidos de utilizar e tratar qualquer dado pessoal contido dentro de sua estrutura, até que a vulnerabilidade seja resolvida por completo e a infração regularizada.

4.5.3 Advertência

Considerada a forma mais branda de penalização, na qual o controlador e o operador receberão por escrito uma advertência com prazo para adequação à legislação. Caso a adequação não seja realizada durante o prazo estipulado, será aplicada uma nova forma de penalização.

4.5.4 Publicização da infração

Neste caso de penalização, após confirmada a ocorrência, o controlador deverá tornar público o vazamento dos dados pessoais, informando o ocorrido em mídias como radio, tv aberta ou jornais. Os impactos dessa penalização estão relacionados à imagem da empresa perante os consumidores.

4.5.5 Multa de até 2% do faturamento com teto máximo de R$ 50 milhões

A multa será aplicada sobre o faturamento no seu último ano, excluídos os tributos, da empresa responsável pela violação dos dados pessoais, sendo de até 2% do faturamento com teto máximo de R$50.000.000,00 reais. Essa penalização é aplicada às organizações públicas ou privadas no Brasil.

Conforme a LGPD, é possível verificar o cálculo do valor da multa a ser paga.

> § 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea. (BRASIL, 2018, np).

4.5.6 Multa diária

A multa diária ocorre até que o problema causador da violação dos dados pessoais seja resolvido por sua totalidade e até que as consequências geradas a partir da violação desses dados sejam minimizadas, através de todos os esforços disponíveis. A multa diária poderá atingir o teto máximo de R$50.000.000,00, conforme mencionado no item 4.5.5.

4.5.7 Suspensão parcial do funcionamento do banco de dados

Esta suspensão refere-se apenas a uma parte do tratamento de dados realizado pelo controlador. Pode ocorrer dentro de 6 meses, possibilitando a prorrogação por período igual, até que exista a regularização do tratamento de dados, ou seja, a correção das vulnerabilidades existentes.

4.5.8 Suspensão do tratamento de dados pessoais

Nesta sanção administrativa, o controlador terá todo o tratamento de dados suspenso. Neste caso, a suspensão pode ocorrer no período máximo de 6 meses, possibilitando a prorrogação por período igual, até que exista a regularização do tratamento de dados, ou seja, a correção das vulnerabilidades existentes.

4.5.9 Proibição parcial ou total no tratamento de dados pessoais

A proibição total pode acarretar falência do controlador, que fica proibido de executar qualquer tipo de tratamento com dados pessoais. No caso de ocorrer a proibição parcial, no entanto, apenas alguns processos são limitados.

Convém ressaltar que as sanções descritas nos itens 4.5.7, 4.5.8 e 4.5.9 só serão aplicadas quando já existir outras sanções, como eliminação dos dados pessoais, bloqueio do tratamento dos dados para qualquer titular, publicização da infração, multa simples e multa diárias, ou quando o controlador for submetido a outros órgãos ou entendidas com competências sancionarias.

4.6 Dosimetria das penalizações

A ANPD irá analisar alguns pontos para medição das penalizações. A forma e a intensidade dessas penalizações serão realizadas de acordo com as medidas preventivas, corretivas ou a falta delas realizadas pelo controlador e operador. Em linhas gerais, quanto mais o controlador e o operador demonstrarem que fizeram o possível, criando medidas técnicas e organizacionais para que não houvesse o vazamento ou minimizassem os impactos causados, menor será a penalização. Contudo, quanto maior o impacto da violação dos dados, maiores serão as penalizações previstas.

Conforme Lei:

> § 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 (...) (BRASIL, 2018, np).

Abaixo, seguem os dez parâmetros e critérios definidos por lei para medição das penalizações que serão aplicadas pela ANPD.

4.6.1 A gravidade e a natureza das infrações

A lei analisa a gravidade da consequência da violação dos dados pessoais, bem como a natureza da infração, ou seja, o local do surgimento dessa infração.

4.6.2 Reincidência

Nesse parâmetro, analisa-se quantas violações de dados pessoais estão envolvidas com esse controlador ou operador e se já houve a reincidência do mesmo tipo de violação de dados pessoais em casos passados.

4.6.3 Boa fé

É analisada se existe boa-fé da organização infratora em relação à violação dos dados pessoais e qual o motivo real dessa violação de dados. Parâmetros, como a cooperação do infrator, ajudam a medição das infrações.

4.6.4 Condição econômica

Será levada em consideração o poder econômico do controlador dos dados pessoais. Quanto maior esse poder, maior será a multa aplicada, isto porque entende-se que controlador com uma condição econômica maior, possui maiores facilidades na aplicabilidade da LGPD.

4.6.5 Proporcionalidade

Neste ponto, será analisada a proporção das consequências geradas após o vazamento dos dados pessoais. Mais uma vez, a criação de planos de ação, podem minimizar as consequências e a proporção que a violação dos dados pode gerar, diminuindo assim as penalizações aplicadas pela ANPD.

4.6.6 Pronta adoção de medidas corretivas

Quanto mais rápida for a adoção de medidas corretivas, menor será a consequência da violação dos dados pessoais ao titular de dados gerando dessa forma, uma penalização menor para o controlador dos dados.

4.6.7 Política de proteção de dados

Neste parâmetro, é verificada a existência de uma política de proteção de dados promovida pela empresa em que houve a violação dos dados pessoais. Entretanto, apenas a existência de uma política não é o único fator a ser verificado, pois não garante que os métodos e processos são aplicados nas ações da empresa como um todo. É necessário que essa política seja aplicada de forma correta e conhecida por todos os colaboradores da organização, bem como existam medidas e processos organizacionais garantindo a utilização dos mesmos.

4.6.8 Política de boas práticas e governança

É verificado a existência e aplicabilidade da política de boas práticas e governança dentro da organização. Como no item anterior, o parâmetro se concretiza tanto com a existência dessas políticas como também com a verificação da aplicabilidade dessas políticas dentro da organização.

4.6.9 Cooperação do infrator

A cooperação da empresa responsável pelo vazamento de dados é fundamental para uma penalização mais branda. Cooperações relacionadas à minimização dos impactos causados, à contenção das informações dos dados que foram violados, entre outras informações, são consideradas ações importantes para a ANPD.

4.6.10 Grau do dano aos titulares

O grau do dano causado pela violação de dados também será utilizado para a medição da penalização. Por esse motivo é importante que exista uma análise prévia dos riscos, bem como um plano de ação, caso ocorra uma violação de dados. Apenas ações rápidas, podem garantir um dano menor, mesmos em casos de dados sensíveis. Além disso, a conscientização dos colaboradores em informar ao DPO de forma rápida também é importante para uma ação de mitigação dos danos.

4.6.11 Vantagem obtida ou pretendida

Neste ponto verifica-se a existência de alguma vantagem obtida ou pretendida que estão relacionadas à violação dos dados pessoais. Caso não exista, as penas serão amenizadas. Apesar das métricas de como a lei será aplicada, muitos pontos ficam em aberto e a lei será aplicada de forma diferente em cada caso de violação de dados pessoais, gerando muitas discussões sobre o assunto. Segundo Santos (2019), é prudente executar a gestão de dados dentro das organizações, para que essas estejam preparadas e não fiquem sob o entendimento do Poder Judiciário, que poderá levar um bom tempo para uma conclusão das disposições da lei. Além do tempo, o Poder Judiciário poderá ter interpretações que não agradam às empresas, trazendo grandes prejuízos às mesmas. Todo o valor arrecadado através multas aplicadas pela ANPD será remetido ao Fundo de Defesa de Direitos Difusos. Esse fundo tem a finalidade de reparar os danos causados ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico.

4.7 O que aconteceu no mundo a partir da criação das leis de proteção de dados

O Brasil não foi o primeiro país a possuir uma lei de proteção de dados pessoais, conforme já descrito. Dessa forma, é possível que seja considerado uma vantagem estar atrás, pois possibilita uma análise do que acontece em outros países onde a lei já está em vigor há algum tempo, permitindo a utilização de lições aprendidas por outros países, a fim de facilitar a aplicabilidade da lei geral de proteção de dados. Conforme Durbano (2020), os países com maior proteção de dados do mundo são os países da união europeia, os Estados Unidos da América, o Japão e a Argentina.

A partir dos dados abaixo é possível verificar que a lei de proteção de dados em outros países tem sido aplicada e cada vez mais difundida entre a população. Isso aponta para a alta probabilidade de que a LGPD no Brasil realmente seja aplicada em sua totalidade, trazendo benefícios e segurança aos dados dos cidadãos brasileiros.

4.7.1 União Europeia

Na União Europeia, muitas multas foram aplicadas durante o primeiro ano. Conforme informação do *site* SegInfo (2020), foram mais de 460 milhões de euros em multa durante o primeiro ano em que a lei entrou em vigor. No primeiro dia em que a GDPR entrou em vigor, segundo o *site* Pedutti Advogados (2019), as plataformas Facebook e Google foram acionadas judicialmente, por não serem transparentes sobre a utilização dos dados pessoais dos usuários de suas plataformas.

Kathrin (2019), por meio do *site* LeadComm, traz dados importantes da associação internacional de profissionais da privacidade. Segundo ela, houve um crescimento nos comunicados de violação de dados pessoais. No primeiro ano, foram registrados cerca de 20 mil casos, já, no segundo ano, o número cresceu para 64 mil relatos de violação de dados. O *site* afirma que este crescimento demonstra a percepção das empresas sobre os benefícios em comunicar o quanto antes uma violação de dados pessoais. Além disso, Incontract (20--) divulgou dados quanto ao conhecimento das pessoas depois de um ano de vigência da GDPR. Esses dados foram informados pela *European Commission* e estão contidos no *site* Incontract (20--, np). São eles:

- 57% dos europeus sabem que existe uma autoridade pública responsável por proteger seus direitos em relação a dados pessoais;
- Foram realizadas 144.376 reclamações às autoridades de proteção de dados europeias por supostas violações à GDPR, principalmente em relação a atividades de telemarketing, e-mails promocionais e vigilância por câmeras de vídeo;
- 89.271 notificações de *data breach* (violação de dados) foram apresentadas por empresas às autoridades europeias de proteção de dados devido à exposição acidental ou ilegal de dados pessoais.

4.7.2 Estados Unidos da América

Nos Estados Unidos, existem várias leis fragmentadas que complementam a questão de privacidade na utilização dos dados pessoais. Mesmo sem uma lei de proteção de dados unificada, para Valente (2018), os Estados Unidos são referência mundial em proteção de dados. Esse país possui a Lei de Privacidade de Comunicação Eletrônica (ECPA), desde 1986, que garante a segurança da informação durante a transmissão e armazenamentos de mensagens, afirma Valente (2018). Além disso, o *autor* cita que o país possuí a Lei de Proteção da Privacidade de crianças (COPPA), algumas normas setoriais, e por fim a lei de privacidade focada nas agências federais. Conforme Gatefy (2020), o governo federal não sinalizou nada a respeito da criação de uma lei única de proteção de dados, mas acredita que

seja o correto para os EUA a criação e a adoção da unificação da lei no país, visto que atualmente existem muitas leis estaduais e federais que envolvem a questão de segurança e privacidade, o que dificulta todo o mapeamento e comunicação entre as regiões. Para Urupá (2020), a lei de privacidade da Califórnia, que começou a valer em 1 de janeiro de 2020 é a mais abrangente dos Estados Unidos, isso porque a lei oferece uma série de alternativas aos residentes no estado da Califórnia, garantindo assim, maior controle na proteção de dados.

4.7.3 Japão

O Japão possui a APPI (*Act on the Protection of Personal Information* – Lei sobre a proteção de informações pessoais). Segundo o site AWS (20--), ela se aplica a todos os operadores, pessoa física e jurídica que tratam dados ou informações pessoais. Durbano (2020) afirma que a primeira lei de proteção de dados no Japão foi criada em 2003 e atualizada posteriormente em 2015 e 2017, um ano antes da GDPR entrar em vigor. Conforme *site* Privacytools (20--), a APPI separa os dados pessoais em duas categorias: informações básicas e informações que requerem cuidados especiais. Além disso, o *site* afirma que entre as penalidades extremas estão as multas e a prisão. O *site* AWS (20--) afirma que em 23 de Janeiro de 2019 a Comissão da União Europeia permitiu a livre circulação dos dados entre as duas economias, pois constataram que Japão e União Europeia possuem fortes garantias de proteção aos dados, o que foi muito positivo para o país.

4.7.4 Argentina

No caso da Argentina, Durbano (2020) informa que o país possui leis específicas para a proteção de dados desde 1994 e atualmente possui em vigor a Lei de Proteção de Dados Pessoais (LDPA), que foi criada a partir do modelo legislativo Europeu e tornou a Argentina o primeiro país da América Latina a se qualificar para transferências de dados à União Europeia. Conforme *site* da Microsoft (2020) a LDPA ou PDPA (*Ley de Protección de los Datos Personales*) está em vigor desde 2000 com o objetivo de proteger os dados pessoais e tem, como responsável pela sua aplicabilidade, o chefe dos Ministérios. Privacytools (20--) afirma que a Argentina está na frente dos demais países da América Latina e aponta também que, de acordo com a comissão Europeia, apenas a Argentina e o Uruguai possuem níveis aceitáveis de proteção de dados.

CAPÍTULO 5: ENTREVISTAS

Neste capítulo será explanado as principais dúvidas em relação à LGPD e que geram grandes discussões sobre a efetividade da lei. Além disso, uma análise no cenário atual das empresas, revelando técnicas utilizadas para a aderência à lei.

5.1 Entrevistas com especialistas

Foram entrevistados dois especialistas sobre a LGPD. O objetivo dessas entrevistas é esclarecer algumas dúvidas a respeito da LGPD existentes na pesquisa. Por se tratar de um assunto novo, não são encontrados muitos materiais sobre a LGPD e essas entrevistas visam completar o entendimento sobre a lei e trazer a esta opinião de especialistas sobre o assunto, conforme as maiores lacunas encontradas na lei. Para tanto, foi realizada uma entrevista estruturada, com respostas abertas, permitindo riqueza nas informações disponibilizadas pelos participantes.

Conforme Coelho (2020), a entrevista é uma técnica importante para coleta de dados subjetivos. Ela afirma que a entrevista estruturada deve ter as perguntas previamente planejadas, o que facilita a captação da opinião dos entrevistados e possibilita a comparação entre as respostas.

O primeiro entrevistado foi o Juan Falguera, que é gerente de Tecnologia na MSTECH em Bauru e tem 13 anos de experiência na área de Governança de TI, infraestrutura *on premisses* e nuvem, além de 10 anos de experiência na área de desenvolvimento de *software* e gerenciamento de projetos. Juan possui certificação em *Data Protection Officer* (DPO) pela AXIN, Certificação em *Information Security* ISO 27001 e Certificação ITIL V3 e atualmente ele exerce a função de DPO dentro da MSTECH.

O segundo entrevistado foi o Juiz Federal do Trabalho Gabriel Lopes Coutinho Filho, que é professor na CEASP - Centro de Estudos Avançados de São Paulo há 5 anos e possui especialização em direito do trabalho, direito processual do trabalho, direito constitucional e direito administrativo.

As perguntas foram encaminhadas previamente via *e-mail* aos participantes e foi permitido que as respostas ocorressem via áudio ou texto devido ao momento de isolamento social. Dessa forma, os participantes preferiram o envio via *e-mail* e as respostas em texto. O questionário enviado encontra-se no Apêndice B.

5.2 Respostas das entrevistas com especialistas

5.2.1 Entrevista com Juan Falguera

Abaixo, o conteúdo na integra da entrevista com Juan Falguera.

1) Um indivíduo que desconhece a LGPD e aceita todos os termos de condições de um determinado controlador sem prestar atenção, pode posteriormente reclamar que seus dados pessoais foram utilizados de forma indevida?

R.: A LGPD estabelece que o controlador deve seguir alguns passos para estar de acordo com a lei. O primeiro deles é obter uma base legal para utilizar os dados pessoais do titular. O consentimento é uma delas. Se o titular deu seu consentimento, então o controlador, já deu seu primeiro passo. No entanto, além da base legal, há 10 princípios que ele deve seguir desde a coleta dos dados até seu descarte, passando pelas diversas formas de tratamento que possa dar a estes dados. Dessa forma, ao apresentar os termos e pedir o consentimento do titular, ele deve fazer isto de forma clara, explícita e objetiva, utilizando linguagem de fácil entendimento. Deve informar a finalidade da coleta dos dados, por quanto tempo os dados ficarão em sua posse, qual a política de proteção de dados que a empresa segue e, se possível, quais os meios que a empresa dispõe para proteger os dados.

Isto tem a ver com alguns dos 10 princípios que o controlador tem de seguir, que são os princípios da transparência, da finalidade, da necessidade e do livre acesso.

Seguindo os 10 princípios, o controlador estará protegido e o titular não poderá reclamar à ANPD que não sabia, pois não leu os termos. Mas apesar de não poder processar o controlador, o titular poderá sempre pedir ao mesmo que revogue seu consentimento e pare de fazer o tratamento de seus dados, pois esse é um dos 10 direitos do titular.

2) De que forma a LGPD pode garantir que a privacidade dos indivíduos seja alcançada, uma vez que se trata também de um direito constitucional?

R.: A lei é muito boa e está em sintonia com as melhores leis de proteção de dados pessoais que existem no mundo. Mas por si só não garante que a privacidade seja alcançada. Como toda a lei, para que seja efetiva, é preciso fiscalização, educação e, em último caso, repressão por meio de multas e outras punições administrativas.

3) Em sua opinião, hoje, no Brasil, nossos dados pessoais estão protegidos?

R.: Sinceramente, hoje, acredito que não. Pelo que tenho visto e conversado com outros profissionais da área, a grande maioria das empresas, principalmente as de médio e

pequeno porte (que são a imensa maioria no Brasil) ainda não se atentaram para os riscos aos quais os dados de seus titulares estão expostos e também aos riscos para seus negócios, que as multas e sanções que a LGPD pode infligir.

As idas e vindas na aprovação e mudança de dados para o início da validade da lei, bem como a demora na criação da ANPD, contribuíram muito para um certo clima de que "a lei não vai pegar". Só que ela já pegou e já está multando algumas empresas.

4) Além da proteção da privacidade, houve outras motivações para a criação da LGPD por parte de nosso Congresso?

R.: É difícil apontar com exatidão as demais motivações, pois não sabemos o que se passa na cabeça de nossos congressistas. No entanto, uma motivação foi tornada pública, não sei se acidentalmente ou não. Foi o fato do Brasil se candidatar a uma vaga na OCDE (Organização para a Cooperação e Desenvolvimento Econômico). É preciso aprovar 245 instrumentos legais que endossem os princípios defendidos pela Organização, sendo que um deles é justamente a proteção de dados pessoais. Entrar na OCDE traria uma série de benefícios a diversas empresas brasileiras.

Além disso, a LGPD europeia (GDPR) estabelece que as empresas pertencentes a UE não pode *a priori* subcontratar ou terceirar atividades que tratem dados pessoais para outras empresas fora da união que tenham sede em países que não possuam leis de proteção de dados. Elas precisariam de uma autorização especial da ANPD europeia para isto, coisa que não é fácil de se obter.

Acredito que estas duas motivações foram suficientes para que grandes empresas brasileiras que tem muito a ganhar ou perder, tenham feito muita pressão sobre nossos congressistas para que aprovassem logo essa lei. Mas isso é só uma suposição de minha parte.

5) Quais as falhas existentes na LGPD no seu entendimento?

R.: Para mim a lei é muito boa e no momento não vejo falhas. Só veremos possíveis falhas quando ela estiver sendo amplamente implementada. Acredito que a falha maior não está na lei, mas em sua regulamentação. A lei só tem o dever de dizer o "que" fazer e isso ela faz bem. Como fazer na prática, é a regulamentação que deveria indicar. E isso é dever da ANPD que ainda não está em pleno funcionamento e demorou muito para ser criada.

6) A base legal "legítimo interesse do controlador" pode ser utilizada em que situação?

R.: Esta é com certeza a base legal mais controversa e que dá muita margem a interpretações. Poderíamos fazer um curso só deste assunto, mas, *a priori*, esta base pode ser utilizada quando o controlador puder alegar que o tratamento dos dados pessoais está sendo realizado como uma extensão de algum produto ou serviço que já foi consumido pelo titular e, portanto, o próprio titular seria beneficiado.

Por exemplo, quando o titular compra um produto em um determinado *site*, o controlador poderia enviar *e-mails* para o titular com promoções de produtos similares. No entanto, o controlador tem de ponderar e fazer um estudo (e registrar este estudo) se os interesses dele não estão sobrepujando os direitos do titular. Se estiverem, outra base legal deverá ser utilizada.

É preciso lembrar que por ser subjetiva, esta base nunca garantirá 100% o cumprimento da lei e, portanto, o controlador deverá pesar este risco e saber conviver com ele.

7) Como ficam os dados de menores de 18 anos, caso o responsável não de consentimento, em bases legais como: interesse vital ou tutela da saúde?

R.: Neste caso, prevalece as bases legais de interesse vital ou tutela da saúde. Não há discussão sobre este ponto, pois preservar a saúde e a vida da criança sobrepõe-se claramente à imposição de consentimento dos pais. Por exemplo, se um médico precisa saber o tipo sanguíneo de uma criança (que é um dado pessoal sensível) para salvar sua vida, é óbvio que não necessita pedir o consentimento dos pais para obter este dado. Mas há outras bases, como "obrigação legal" ou execução de "políticas públicas" que também poderiam dispensar o consentimento dos pais ou responsáveis. Mas nestes casos seria preciso analisar com mais cautela em cada situação.

8) A ANPD funcionará como a ANATEL e receberá reclamações? Todas serão analisadas?

R.: A ideia é mais ou menos esta. A ANPD deveria ter condições de receber e tratar todas as reclamações em um tempo razoável. Se vai conseguir fazer, ainda não sabemos. Na Europa, foram criadas diversas ANPDs regionais, regidas pela ANPD central, mas que tem autonomia para tratar as reclamações e impor multas e sanções.

ANPD poderia também criar algum tipo de convênio com outros órgãos, como o Procon, por exemplo, pra dar conta da demanda. Pode ser que num país tão grande como o nosso, estas sejam soluções viáveis.

9) Como uma pessoa pode ter proteção de dados sem conhecer a LGPD?

R.: A proteção de dados é uma área que faz parte da TI há muito tempo, muito antes da LGPD. Existem cursos e certificados em proteção de dados, homologados pela ISO, que permitem a um profissional conhecer todas as formas de risco aos dados e também as melhores formas de dirimir estes riscos.

Como se sabe, dados pessoais são um subgrupo do conjunto de dados que são coletados, processados e armazenados pelas empresas. Se uma empresa colocar em prática todos os processos previstos na ISO 27000, por exemplo, ela estará protegendo também os dados pessoais e faltará muito pouco para que esteja 100% de acordo com a LGPD.
No entanto, há alguns processos que são exclusivos da LGPD. Portanto, é essencial conhece-la para poder cumprir a lei de forma integral.

5.2.2 Entrevista com Gabriel Lopes Coutinho Filho

Abaixo, expõe-se o conteúdo na integra da entrevista com o Juiz Gabriel Lopes Coutinho Filho.

1) Ao seu entender, a LGPD se aplica aos indivíduos que desconhecem o seu dado como um direito individual? Por exemplo, um indivíduo que desconhece da LGPD e aceita todos os termos de condições e todas as políticas de privacidade.

R.: O desconhecimento de uma lei protetiva não autoriza o aplicador da lei a tirar partido da ignorância do destinatário. Um exemplo simples é a lei de proteção do consumidor. Claro que a correção de uma lesão de direito não se dá automaticamente. Se a pessoa (no caso, o consumidor) desconhece sua lesão ou prejuízo, ou desconhece que certa situação é uma lesão, o sistema jurídico atual não permite, em regra, que um terceiro defenda os direitos dessa pessoa. Ninguém pode postular judicialmente direito de terceiros em um nome próprio. As exceções são os pais ou responsáveis, no plano individual, e o Ministério público ou então órgãos de defesa, no plano coletivo.

Desconhecer os direitos individuais promovidos pela LGPD não implica em não ter respeitado esses direitos desde que aquele que se sente lesado ou prejudicado provoque o judiciário ou algum órgão de defesa para corrigir a lesão.

A norma tenta, de alguma forma, também colaborar com a educação do cidadão (formação da cidadania) e isso nós verificamos com a exposição que esse tema tem alcançado na mídia atualmente.

A noção de “consentimento” (bem como o de “legitimo interesse”) para acesso aos dados pessoais ainda é incipiente, mas, com o tempo, as pessoas começarão a entender como esse “consentimento ” é relevante e que a exata noção de ter essa autorização deve ser livre e esclarecida, consciente de suas repercussões, direitos e responsabilidades. Só assim, mediante e exigência de cumprimento da lei, é que os atores econômicos se preocuparão em fazer esse “consentimento” refletir a vontade do legislador. Por isso é importante a educação das pessoas inclusive para que e elas procurem defender adequadamente seus direitos e que comecem a existir punições efetivas para aqueles que desrespeitam a privacidade dos dados pessoais, fazendo mau uso deles.

Se o consentimento é dado pelo consumidor/usuário sem efetivo esclarecimento ou então que os dados pessoais sejam utilizados contra quem os concede (sem um “legitimo interesse”), naturalmente este consentimento não tem valor e, portanto, não terá efeito prático. Quem, como empresa, faz uso incorreto do consentimento não obterá o efetivo direito de utilizar os dados pessoais de seus clientes ou usuários; e estará vulnerável a responder legalmente. Em síntese: não deve ser motivo de real preocupação concordar com “termos de consentimentos” que não estejam de acordo com a lei; isso se traduz em mais uma camada de proteção para o consumidor e o próprio cidadão.

Para que a posição não seja mal compreendida, deixo claro que toda atenção a termos de consentimento é importante e economiza esforço daquela pessoa que for lesada, prejudicada ou “enganada”. Quanto mais nós temos ciência dos nossos direitos, maior e melhor se torna a nossa vigilância e proteção contra possíveis ataques.

2) Conforme artigo da constituição, que prevê a privacidade como um direito, é possível alcançar a privacidade com a LGPD?

R.: A LGPD é uma norma muito recente, que acompanha seu tempo, e seus conceitos e aplicação serão aperfeiçoados com o tempo. Podemos entender que o conceito de privacidade também vai mudar conforme o avanço das tecnologias de informação. Até poucos anos não tínhamos noção dos efeitos do uso de nossos dados pessoais postos voluntariamente na internet. Hoje, já sabemos como o uso desses dados podem nos prejudicar. Com certeza, novos mecanismos de captura e utilização de dados pessoais poderão surgir. A lei indica conceitos e direitos que irão se ampliar na sua boa aplicação.

Concorrente com o que apresentamos na questão anterior, um direito deve ser concretizado, ou seja, não adianta estar previsto em uma norma, mas não ser respeitado. Nenhuma lei, sozinha, será efetiva se não houver defesa de sua aplicação. Privacidade com

dados pessoais, como valor essencial, já possui um amparo legal no Brasil com a LGPD. Mas sempre precisará ser defendida, caso contrário torna-se letra morta e alvo fácil para agentes econômicos sem ética ou que não respeitem a lei.

3) Em sua opinião, nossos dados estão protegidos?

R.: Não, nossos dados não estão protegidos. Pelo menos não estão protegidos como deveriam. Não é difícil encontrar na internet pesquisas informando o nível de empresas que já aderiram à LGPD. E podemos, com base nessas pesquisas , prognosticar o que ainda levará tempo para que a cobertura de privacidade dos dados pessoais tenha um bom índice. Há empresas que sequer sabem minimamente suas obrigações na LGPD e que tratam nossos dados sem maiores cuidados. O problema que precisaremos entender é que o atual modelo de negócios da internet, que várias vezes proporciona algum tipo de serviço “gratuito” em troca de valiosos dados pessoais, é bastante prejudicial.

Vamos usar como exemplo os serviços de buscas do Google: ainda não temos a cultura de pagar por um serviço de buscas que entendemos como gratuito e que, na verdade, oferece muito pouco pela vastidão e profundidade riqueza de dados pessoais que recolhe. Levará tempo para que esse modelo de negócios seja alterado, especialmente ao ponto de beneficiar o consumidor/cidadão.

4) Qual o real motivo da criação da LGPD?

R.: Um primeiro motivo é a percepção, especialmente dos cidadãos europeus e americanos, da agressão representada pela colheita de dados pessoais sem autorização e o quanto isso significa de invasão de privacidade por parte, principalmente, das grandes empresas de internet. A segunda percepção, concorrente, vem do prejuízo manifesto para o cidadão/consumidor que tem seus dados pessoais colhidos sem consentimento, comercializados ou então utilizados contra seus interesses e propósitos. Uma terceira percepção advém do potencial de uso político irregular que o acesso e tratamento de dados pessoais podem significar no plano nacional e internacional.

Seria possível ainda estabelecer que a internet através da colheita de dados pessoais sem consentimento elevou suas ações a um nível surpreendente de monetização da atividade, com concentração de riquezas incomparáveis e o potencial de lucratividade dos negócios digitais.

5) Quais as falhas existentes na LGPD ao seu entender?

R.: A bem da verdade, a falha não está especificamente na LGPD, mas na lei processual civil. O projeto de lei do código de processo civil (CPC) em vigor preferia a conversão de ações individuais com interesses coletivos em "ações coletivas", aquilo que o sistema americano chama de "*class actions*". Esse mecanismo poderia ter modificado em muito o panorama geral não só da lei de proteção de dados, mas diversos outros direitos "meta individuais" ou coletivos. Imagine uma ação individual discutindo tarifas bancárias, se transformada em ação coletiva, beneficiando todos os consumidores de serviços bancários. O mesmo para discussões sobre tarifas de telefone celulares, serviços de internet, de TV a cabo, ou então, ações individuais de mandando por água e luz em bairros menos favorecidos, ponto de ações contra poluição, serviços públicos essenciais. Enfim, a substituição de ações judiciais individuais em massa por ações coletivas, poucas, que resolvessem em massa grandes problemas da sociedade. Perdemos uma grande chance de transformação social.

Relativo à lei em si, particularmente acho que vai gerar muita dúvida a questão de sua aplicação territorial tem como a competência para tratamento de dados em um mundo cada vez mais sem fronteiras e com *players* transnacionais.

6) Legítimo interesse pode ser utilizado em que situação?

R.: Junto com o consentimento livre, o legitimo interesse é um dos pilares da LGPD. Se uma empresa desejar fazer o tratamento de dados pessoais de seus clientes ou das pessoas com quem se relaciona, a legitimidade do interesse se caracteriza pela explicação adequada em extensão e profundidade daquilo que será feito com esses dados colhidos e tratados. O legitimo interesse do uso de um dado pessoal é questão formal e auditável, demonstrável nas razões pelas quais o tratamento da informação é feito e usado. A decorrência lógica desse legítimo interesse é a sua legítima utilização, que também deve ser demonstrável, comprovada nos termos da lei.

Uma empresa que recolher dados de saúde de seus empregados pode ter o legitimo interesse de protegê-los de produtos tóxicos; todavia, não terá legitimo interesse se repassar essas informações para empresas de seguro saúde. Ainda na área de saúde, que é uma questão sensível, um pedido de mapeamento genético para o empregado, à primeira vista, parece ser totalmente ilegítimo, salvo se houver um interesse claro, transparente e fundamentado de tal requerimento, pois um mapeamento genético é de grande valor financeiro e estratégico para as empresas que fornecem seguro saúde.

Informações pessoais também na área financeira são de grande atratividade; um banco, por exemplo, só terá interesse em conhecer o seu potencial financeiro se desejar oferecer

serviços dos quais você, de antemão, deve saber como algum detalhamento; deve se ter muito cuidado ao fornecer, por exemplo, cópia da sua declaração anual de ajuste de imposto de renda a um banco ou agente financeiro.

O legitimo interesse e o consentimento livre e consciente, como pilares da LGPD, são duas grandes "bússolas" para qualquer consumidor cidadão decidir com razoabilidade se autoriza ou não o acesso de um interessado aos seus dados pessoais.

7) Como ficam os dados de menores de 18 anos, caso o responsável não de consentimento, em bases legais como: interesse vital ou tutela da saúde?

R.:O menor de 18 anos não tem capacidade civil para autorizar o tratamento dos seus dados pessoais, salvo com consentimento dos responsáveis, nos termos da LGPD. Todavia, na hipótese de necessidade do dado pessoal para cumprimento de lei, como é o caso do registro de menor, o empregador tem legitimo interesse, tem razão da necessidade dos dados por obrigação legal. Por parte do empregador, deve haver redobrada atenção para a requisição e tratamento de dados pessoais de menores que sejam estritamente necessários para o cumprimento da lei.

Na hipótese de acidentes em que o menor esteja envolvido e precise de atendimento médico, o valor "vida" e "saúde" naturalmente assumem uma importância diferenciada e relevante, que afasta o impedimento legal. Nessas circunstâncias excepcionais, é razoável que a empresa, que faz esse tratamento de dados, tenha cuidados adicionais documentais e testemunhais para eventual comprovação da necessidade de colheita e tratamento do dado do menor.

8) A ANPD funcionará como a ANATEL e receberá reclamações? Todas serão analisadas?

R.: Pela norma em vigor, a ANPD receberá reclamações especialmente de vazamento de dados pessoais restando, entre suas competências, a apuração de responsabilidades e até a aplicação de multas administrativas que poderão ir até 50 milhões de reais ou 2% do faturamento. A agência ainda está em processo de estruturação e o atendimento e a análise de todas as reclamações e outras providências dependerão dessa estrutura administrativa ainda não terminada.

É interessante lembrar o que o Supremo Tribunal Federal (STF) já decidiu que não há necessidade de percorrer as vias administrativas para reclamações em agências de regulação,

especialmente nas hipóteses em que o órgão não dá resposta suficiente em qualidade e prazo razoável, como pressuposto de judicialização de questões envolvendo suas competências.

9) Como uma pessoa pode ter proteção de dados sem conhecer a LGPD?

R.: Com a difusão da LGPD, é lícito presumir que as empresas tenderão a aplicar a legislação e, dessa forma, as pessoas estarão protegidas em algum grau. Mas é claro que o conhecimento da norma aumenta a capacidade de resistência, de proteção, e da adoção de eventuais providências de defesa.

Guardada a devida proporção, é o mesmo que se observa com a lei de proteção do consumidor. Imaginemos quantos consumidores não são lesados por empresas que atuam não observando mínimos padrões de ética ou mesmo padrões legais. Mesmo o consumidor não conhecendo seus direitos ele os possui. É importante lembrar que somente ele, consumidor, como interessado, é que poderá reagir e tomar providências cabíveis, tal como reclamação aos órgãos de proteção ou a judicialização da questão. O mesmo ocorrerá com as situações envolvendo a LGPD.

5.3 Momento atual das empresas

Desde agosto de 2018, uma grande movimentação vem ocorrendo dentro das organizações. A LGPD trouxe consigo muitas mudanças de paradigmas e inclusive culturais que precisaram ser estudadas e aplicadas, o que demanda um tempo alto e investimentos dentro das organizações. O desafio foi e continua muito grande dentro das organizações, que não podem parar suas tarefas e processos diários e precisam incluir em seu escopo a aplicabilidade da LGPD. Para facilitar o entendimento da lei, foram trazidas algumas informações sobre a aplicabilidade dela em empresas diversas, porém, por motivo de sigilo, os dados da empresa não serão revelados. Essas empresas possuem um conteúdo relevante com passos e dicas para a aplicabilidade da LGPD. Após a publicação da lei, os primeiros passos foram iniciados, contanto com a realização de muitos cursos aplicados aos colaboradores, com o intuito de disseminar o conhecimento sobre o processo e os deveres da empresa. A disseminação do conhecimento foi o primeiro passo da aplicabilidade da LGPD, porém muitos problemas ainda são encontrados nesse ponto, com algumas dúvidas gerais sobre a implementação da LGPD, que somente serão sanadas após a consolidação da ANPD. Após o conhecimento dessa lei por todos os colaboradores, foi realizado uma análise do cenário atual da organização, criando uma planilha de identificação dos dados pessoais tratados em cada uma das áreas da empresa. Essa planilha é conhecida como o mapa de dados

pessoais, no qual estão relacionados os dados pessoais identificados com os princípios da LGPD em cada uma das áreas da empresa.

Abaixo, mostra-se um modelo de planilha utilizado na criação do mapeamento dos dados pessoais, identificando os dados tratados pela organização.

	Informação Pessoal	Titular dos Dados	Bases para o Processamento	Processamento de Dados	Acesso	Descarte	Tipo de comunicação	Consentimento
Como o dado foi coletado?	Quais informações pessoais você está coletando?	Como o titular está lhe provendo os dados?	Por que você está coletando os dados?	Explique como você está armazenando os dados e como eles serão processados	Quem tem acesso aos dados e por quê?	Quando os dados serão descartados?	Qual o tipo de comunicação utilizado para tratar com o Titular?	Como você obteve o consentimento?

Figura 22 - Mapa de dados pessoais
Fonte: Paraschiv (2018).

Após o mapeamento dos dados pessoais, foi realizada a avaliação de impacto sobre a proteção de dados pessoais. Essa avaliação é conhecida como AIPD. A AIPD está alinhada aos princípios de proteção de dados *by design* e avalia principalmente a necessidade de cada dado, a proporcionalidade que causará caso um dado seja vazado e os riscos de vazamento de cada um desses dados.

A AIPD não é obrigatória no Brasil, porém na União Europeia tem seu uso obrigatório para os dados sensíveis e deve ser executada sempre que houver mudanças dentro dos processos organizacionais. Além disso, ela deve conter a avalição e medida de mitigação para os riscos associados a:

- finalidade de processamento;
- limitação/ retenção de dados;
- localização e transferência;
- direitos dos titulares de dados;
- bases legais.

Abaixo, segue um modelo da planilha AIPD e como deve ser preenchida.

Assunto	Avaliação de Riscos	Medidas de Mitigação	Conclusão
•Finalidade de processamento	Equipes internas podem utilizar dados diferentemente do acordado com o titular.	Capacitar as equipes internas sobre a LGPD.	Risco suficientemente mitigado.
•Limitação/Retenção de dados	Os dados coletados ficam armazenados por um tempo desnecessário à finalidade.	Criar um processo para exclusão dos dados após o seu processamento.	Risco suficientemente mitigado.
•Localização e transferência			
•Direitos dos Titulares de Dados			
•Bases Legais			

Figura 23 - Modelo AIPD – Avaliação de impacto sobre a proteção de dados
Fonte: Próprio autor.

Após o preenchimento e levantamento dos dados pessoais tratados dentro da organização, o momento foi utilizado para revisão e adequação de todos os processos existentes. Abaixo, expõe-se os principais itens que foram indicados no processo da organização:

- ➔ Operadores
  - Revisão dos contratos com prestadores de serviços. A partir dessa ação foram incluídas clausulas sobre o que pode ou não ser feito com cada dado pessoal disponibilizado;
  - Revisão dos dados pessoais disponibilizados à prestadores de serviços e a áreas dentro da organização, com a finalidade de minimizar os dados que são compartilhados entre as diversas áreas da organização;
  - Revisão dos termos de NDA de funcionários, incluindo clausulas especificas sobre a privacidade dos dados tratados pelos colaboradores.
- ➔ Captação de dados
  - Revisão de contratos e termos de adesão especificando as finalidades para captação de dados pessoais, a forma de armazenamento e o tempo de retenção para cada dado coletado;
  - Adaptação dos dados que são captados, minimizando a coleta dessas informações, ou seja, apenas dados com necessidade específica para os fins serão solicitados ao titular de dados;
  - Para a captação de *leads* para marketing digital, foi necessária a adaptação dos sistemas para que exista a opção *opt-in*, ou seja, o usuário precisa clicar permitindo o recebimento dessas propagandas. Captação através de sistema

opt-out foi retirada. Ela ocorria quando, ao realizar o preenchimento de um formulário, a opção de receber propaganda já vinha pré-selecionada, infringindo dessa forma os princípios da LGPD.

➔ Revisão de sistemas

- Os sistemas que armazenam os dados pessoais foram revisados, garantido que esse armazenamento seja seguro;
- Os dados sensíveis necessários para tratamento foram criptografados;
- A disponibilização dos direitos do titular dos dados ocorreu, ou seja, foram criadas formas de disponibilizar os direitos ao titular de dados pelos operadores quando houver solicitação por parte do titular dos dados. Para isso, houve alterações de sistemas, disponibilizando esses direitos previstos em lei.

No geral, foram diversos pontos analisados e muitas mudanças em processos, documentos e sistemas. Algumas consultorias especializadas na implantação da LGPD continuam ajudando nesse processo de mapeamento e adequação à nova LGPD, criando relatórios de impactos em privacidade e proteção de dados. Essas consultorias auxiliam na identificação dos pontos falhos e na forma mais adequada para adaptação. O processo na empresa analisada ainda não foi finalizado, porém já existe muitos pontos em conformidades com a nova lei.

Essa empresa é um *case* que está muito adiantado em relação à implementação da LGPD. Muitas outras organizações ainda não conhecem o que é a nova lei de proteção de dados e outras ainda não se conscientizaram de toda adaptação que deve ocorrer dentro de sua estrutura, para que a lei seja aplicada. É comum verificar empresas ainda no início deste processo, apesar da lei já estar em vigor desde setembro de 2020. O desconhecimento sobre a LGPD é ainda realidade de muitas organizações. Além disso, necessita de um investimento em tempo e dinheiro para sua aplicabilidade, o que está cada vez mais distante, principalmente em um ano, no qual a pandemia do novo Coronavirus, causou grandes impactos nos negócios e no faturamento de muitas empresas. Com isso, a LGPD continua não aplicável em diversas organizações brasileiras.

CAPÍTULO 6: CONSIDERAÇÕES FINAIS

O objetivo principal desta pesquisa foi analisar a lei vigente de proteção de dados pessoais (LGPD) no Brasil e suas implicações na relação entre empresas e usuários no ambiente virtual, trazendo informações relevantes sobre a lei, criando um guia para a sociedade brasileira.

O primeiro passo foi realizado ao aplicar o questionário no início desta pesquisa, visto que ele foi utilizado como embasamento para a validação da necessidade do trabalho. Por meio desta pesquisa, ficou evidente a lacuna existente entre o direito e o saber, notando-se a falta de conhecimento dos indivíduos sobre o direito individual de cada pessoa, motivo que cria essa separação. Com base nisso, percebe-se que mesmo com leis vigentes para a proteção de dados, os indivíduos não estão protegidos, pois não conhecem seus direitos. Dessa forma, destaca-se aqui que todo o estudo visou reunir o conhecimento necessário sobre a nova lei de proteção de dados, seus impactos e sua aplicabilidade nas organizações na atualidade. Portanto, este estudo levou à reflexão final sobre a necessidade de uma educação tecnológica aparando as arestas existentes entre o conhecimento da sociedade e os direitos dos cidadãos.

Partindo dessa confirmação, esta pesquisa iniciou-se com uma contextualização sobre as informações tratadas dentro das organizações. Foi identificado que as informações somente conseguem ter um valor, a partir do momento que são categorizadas e classificadas em grupos, gerando assim, o conhecimento desejado pelas organizações. Assim, após a coleta de dados pessoais existe um processo que transforma os dados em informação, e a partir desse momento, os mesmos se tornam vitais para as empresas, permitindo-a traçar alternativas de sobrevivência em uma sociedade competitiva, tornando-se mais valiosa para o âmbito corporativo.

O estudo bibliográfico apontou a existência de cidadãos que cedem suas informações para as organizações em troca da utilização ou aquisição de um serviço, no entanto eles possuem direitos à privacidade, conforme a Constituição Federal de 1988, art5, inciso X. Além dos direitos existentes sobre a privacidade, foi observado ainda sobre o direito individual de cada cidadão, que permite a transferência desses dados e sua utilização por terceiros, no momento que achar oportuno, muitas vezes por desconhecer os riscos envolvidos na utilização dos seus dados pessoais.

Após toda a contextualização, estudou-se a nova Lei geral de proteção de dados – LGPD, que entrou em vigor em setembro de 2020 e que complementou o Marco Civil da internet. A LGPD trouxe uma tentativa de garantir a privacidade aos indivíduos, através de

métodos e técnicas de proteção de dados, permitindo a cada titular direitos específicos sobre os seus dados e garantindo a utilização dos mesmos pelas organizações, apenas para finalidades informadas de forma clara e transparente. Além disso, é importante ressaltar que a estrutura da nova lei inclui 65 artigos que foram agrupados nas: dez bases legais, que são os motivos legítimos para o tratamento dos dados pessoais; nos dez princípios e regras que precisam ser seguidas pelos controladores de dados no momento do tratamento dos dados pessoais, a fim de proteger os dados confiados pelo titular e por último os oito direitos concedidos ao titular de dados relativos aos dados tratados pelo controlador. A lei aplica-se a quem realiza tratamento de dados pessoais para fins comerciais, independente do meio e forma de tratamento desses dados. Dessa forma, é possível concluir que para outros tipos de tratamento a lei não se aplica, deixando lacunas na questão da proteção dos dados pessoais.

Por último, foram investigados os impactos gerados com a nova lei na sociedade e ficou perceptível que ainda existe uma busca por soluções para a criação de uma cultura organizacional, na qual a proteção de dados seja vista como prioridade dentro das organizações. A adequação das empresas gerou um grande custo operacional, aumentando o quadro de colaboradores e criando novas funções para suprir as exigências. Atualmente as empresas no Brasil ainda buscam a adaptação às normativas da nova lei, utilizando de ferramentas como o Mapa de dados pessoais e a avaliação de impacto sobre a proteção de dados, para mapear todo o processo que precisa ser revisado e alterado. Além disso, foi verificado que a criação de programas de *Compliance* e de governança tem auxiliado na criação de novos processos, para a adequação às novas normativas que a LGPD dispõe. Complementando este cenário, muitas empresas de consultoria em LGPD foram envolvidas no meio corporativo, que ainda busca aderência à nova lei.

As penalizações previstas por lei são severas e podem gerar um grande impacto financeiro, como multas de até R$50.000.000,00 reais, ou também um impacto na reputação da empresa, no caso de publicização da infração. Essas penalizações são medidas a partir de critérios definidos em lei, relacionados ao esforço realizado pela empresa em se adaptar às novas normativas, bem como nas medidas tomadas para evitar a violação de dados pessoais e no auxilio prestado pelas organizações no caso de uma possível violação de dados pessoais.

Paralelamente, durante o estudo realizado, foram identificadas lacunas existentes na interpretação da lei e dúvidas foram levantadas em diversos cursos ministrados pelo autor desta pesquisa. Dessa forma, essas dúvidas foram reunidas, criando assim, uma entrevista estruturada e aplicada a dois especialistas no assunto, com a finalidade de minimizar esses

pontos existentes de dúvidas. Essas entrevistas trouxeram informações relevantes sobre o assunto, minimizando as discussões existentes.

É importante salientar que esta pesquisa não teve como objetivo o estudo da privacidade em si e as ferramentas utilizadas para a captação de dados, e sim uma análise sobre nova legislação brasileira de proteção de dados e o momento atual de uso de dados, referindo-se ao processo inicial de um estudo que possui muitas vertentes e faz parte de um assunto dinâmico, que ainda se encontra no início de sua trajetória. Além disso, essa pesquisa possibilitou a criação de um material inicial como base para outros pesquisadores.

Após todo o processo de pesquisa houve um crescimento no entendimento da LGPD, bem como o aprimoramento da escrita e do desenvolvimento das ideias relacionadas à proteção de dados. Concluindo-se que mesmo diante da movimentação de transformação da privacidade sendo interpretada atualmente como um bem jurídico em busca da proteção dos dados pessoais, existe cidadãos com direitos individuais que desconhecem todo esse processo e principalmente os seus direitos. A LGPD obriga que as empresas realizem todos os esforços necessários com a finalidade de garantir a privacidade das pessoas físicas. Para atingir esse objetivo, foi necessário que as organizações solicitassem o consentimento aos titulares de dados. Em casos que as empresas não possuam uma das nove bases legais para tratamento desses dados pessoais, se houver o consentimento do Titular, as empresas estarão em conformidade com a nova lei, possibilitando o tratamento para fins diversos, inclusive para a utilização desses dados como ferramentas para o processo decisório e direcional das organizações. Porém, o consentimento causou um impacto grande nas empresas, por ser um processo trabalhoso e por garantir o direito de sua revogação por parte do titular a qualquer momento.

Dessa forma, é importante ressaltar que a Lei geral de proteção de dados não resolve todos os problemas relacionados à proteção de dados. Além da existência da lei, é relevante que cada cidadão conheça seus direitos e os deveres dos controladores de dados, a quem seus dados são confiados, além de entender como cada informação pode ser importante para as tomadas de decisões garantindo que a escolha entre fornecer ou não seus dados pessoais, seja baseada em uma decisão consciente. O direito apenas pode ser aplicado quando houver o conhecimento de que existe uma regulamentação vigente. Em contra partida, a lei apenas é aplicada para fins comerciais, não regulamentando outros tipos de tratamento de dados que continuam vulneráveis e que poderão causar prejuízos e ameaças no modo de viver dessas pessoas. Acima de tudo, vale ressaltar que com a inserção da tecnologia na sociedade em todos os momentos, a educação tecnológica passa a ser fundamental para a construção de uma

sociedade que toma as decisões corretas sobre a utilização de seus dados, não sendo apenas por impulso e sim pela necessidade, transformando os cidadãos em pessoas críticas de suas escolhas.

REFERÊNCIAS

ALVES, P. O que são cookies? Entenda os dados que os sites guardam sobre você: entenda o que são esses elementos conhecidos da Internet e como podem ser benéficos ou prejudiciais ao usuário. In: **Techtudo**. 04 out. 2018. Disponível em: https:www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml. Acesso em: 24 jan. 2021.

BORTOLI. J. de. Data Mining – (Mineração de dados). In: **Joel de Bortoli** – blog. 17 ago. 2012. Disponível em: https://www.joeldebortoli.com/2012/08/data-mining-mineracao-de-dados.html. Acesso em: 08 jun. 2020.

Brasil é o país mais propenso a sofrer vazamentos de dados em todo o mundo. In: **TECMUNDO.** 27 jun. 2020. Disponível em: https://www.tecmundo.com.br/seguranca/154520-brasil-pais-propenso-sofrer-vazamento-o-mundo.htm. Acesso em: 14 jan. 2021.

BRASIL. Constituição de 1988. **Constituição da República Federativa do Brasil**. Brasília, DF: Câmara dos Deputados, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jan. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a lei geral de proteção de dados pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 set. 2020.

CASTRO. G. R. de. **Discussão conceitual sobre dado, informação e conhecimento**: perspectiva dos alunos concluintes do curso de biblioteconomia da UFPB. 2011. Monografia (Trabalho de Conclusão da Graduação em Biblioteconomia – Universidade Federal da Paraíba, João Pessoa, 2011. Disponível em: https://security.ufpb.br/biblio/contents/tcc/tcc-2011/discussao-conceitual-sobre-dado-informacao-e-conhecimento.pdf. Acesso em: 20 out. 2020.

CETAX. Big data: o que é, conceito e definição. In: **Data analytics, big data, data science – blog cetax**: artigos, materiais e tutoriais de business intelligence, big data, data warehouse e etl. 07 ago. 2020. Disponível em: https://www.cetax.com.br/blog/big-data/. Acesso em: 23 jan. 2021.

CHIAVENATO, I. **Introdução à teoria geral da administração.** 6º edição. Rio de Janeiro: Campus, 2000.

COELHO, Beatriz. Entrevista: técnica de coleta de dados em pesquisa qualitativa. In: **Mettzer**. Florianópolis, 30 out. 2020. Disponível em: https://blog.mettzer.com/entrevista-pesquisa-qualitativa/. Acesso em: 17 jan. 2021.

Como funcionam as leis de proteção de dados nos Estados Unidos. In: **Gatefy**. 20 jan. 2020. Disponível em: https://gatefy.com/pt-br/blog/como-funcionam-leis-protecao-dados-estados-unidos/. Acesso em: 04 jan. 2021.

Como o Brasil e outros países estão protegendo os dados dos cidadãos? In: **Ideação**: inovação em gestão pública. 30 abr. 2019. Disponível em: https://blogs.iadb.org/brasil/pt-br/como-o-brasil-e-outros-paises-estao-protegendo-os-dados-dos-cidadaos/. Acesso em: 30 set. 2020.

Conhecimento. **Dicio**, Dicionário online de português, definições e significados de mais de 400 mil palavras. 2021. Disponível em: https://www.dicio.com.br/conhecimento/. Acesso em: 30 jan. 2021.

Conheça as multas já aplicadas por violação no tratamento de dados pessoais e entenda porquê. In: **Peduti Advogados**: propriedade intelectual. 27 fev. 2019. Disponível em: https://peduti.com.br/blog/multas-ja-aplicadas-pelo-gdpr/. Acesso em: 16 set. 2020.

COSTA, M. M. da. **A era da vigilância no ciberespaço e os impactos da nova lei geral de proteção de dados pessoais no brasil**: reflexos no direito à privacidade. 2018. Monografia (Trabalho de Conclusão do Curso de Graduação em Direito – Faculdade de Direito da Universidade Federal do Rio de Janeiro , Rio de Janeiro, 2018. Disponível em: https://pantheon.ufrj.br/handle/11422/8252. Acesso em: 31 ago. 2019.

Cultura. **Dicio**, Dicionário online de português, definições e significados de mais de 400 mil palavras. 2021. Disponível em: https://www.dicio.com.br/cultura/. Acesso em: 30 jan. 2021

Cyrela é multada em R$ 10 mil por infração à Lei Geral de Proteção de Dados: decisão é uma das primeiras referentes à nova lei, que entrou em vigor no dia 18. **G1**, Valor online. 30 set. 2020. Disponível em: https://g1.globo.com/economia/noticia/2020/09/30/cyrela-e-multada-em-r-10-mil-por-infracao-a-lei-geral-de-protecao-de-dados.ghtml. Acesso em: 19 dez. 2020.

DONELLA, G. Compliance: descubra o significado desse conceito e por que sua aplicação é crucial dentro das empresas. In: **Capital aberto**: o mercado de capitais sobre novos ângulos. 10 maio 2019. Disponível em: https://capitalaberto.com.br/secoes/explicando/o-que-e-compliance/. Acesso em: 04 jan. 2021.

DURBANO, V. Leis de proteção de dados pelo mundo: como aplicar a devida prioridade e importância dos dados pessoais. In: **Ecoit**: segurança digital. São Paulo, mar. 2020. Disponível em: https://blog.ecoit.com.br/leis-de-protecao-de-dados-pelo-mundo-como-aplicar-a-devida-prioridade-e-importancia-dos-dados-pessoais/. Acesso em: 10 out. 2020.

Entenda o que é *compliance* nas empresas e a importância desse conceito. In: **Siteware**. 27 nov. 2017. Disponível em: https://www.siteware.com.br/blog/processos/o-que-e-compliance-nas-empresas/ Acesso em: 11 de dez. 2020.

Entenda o que é *data mining* suas aplicações e como funciona a mineração de dados. In: **Rockcontent**. 7 jan. 2020. Disponível em: https://rockcontent.com/br/blog/data-mining/. Acesso em: 28 dez. 2020.

Evite multas e transtornos adequando seu site à LGPD. In: **C3dweb**. [20—]. Disponível em: https://www.c3dweb.com.br/blog/marketing-digital/evite-multas-e-transtornos-adequando-

seu-site-a-lgpd/#:~:text=Se%20n%C3%A3o%20cumprirem%2C%20elas%20ser%C3%A3o,com%20uma%20configura%C3%A7%C3%A3o%20mais%20dura. Acesso em: 13 nov. 2020.

FEBRABAN, Federação Brasileira de Bancos. **Pesquisa FEBRABAN de Tecnologia Bancária 2019.** 2019. Disponível em: https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf. Acesso em: 20 set. 2020.

FERREIRA. A. O valor dos dados. In: **Oper blog**. Belo Horizonte, 09 ago. 2019. Disponível em: https://operdata.com.br/blog/o-valor-dos-dados/#:~:text=Dados%20s%C3%A3o%20capazes%20de%20gerar,gera%20energia%20e%20produtos%20f%C3%ADsicos. Acesso em: 14 jan. 2021.

FREIRE, R. O que é Oversharing? In: **Techtudo**. 18 jan. 2015. Disponível em: https://www.techtudo.com.br/noticias/noticia/2015/01/o-que-e-oversharing.html#:~:text=Compartilhar%20exageradamente%3A%20essa%20%C3%A9%20a%20ideia%20por%20tr%C3%A1s%20do%20oversharing.. Acesso em: 07 out. 2020.

FUGAZZA, G. Q.; SALDANHA, G. S. Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais. **Encontros Bibli**: revista eletrônica de biblioteconomia e ciência da informação, Florianópolis, v. 22, n.50, p. 91-101, 2017. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2017v22n50p91/34697. Acesso em: 05 out. 2019.

GARRUTE, M. M.; SCHMIDT, E. A violação de dados pessoais e seus impactos sob a égide do Regulamento Europeu de Proteção de Dados (GDPR). In: **Migalhas**. 24 jan. 2020. Disponível em: https://migalhas.uol.com.br/depeso/319059/a-violacao-de-dados-pessoais-e-seus-impactos-sob-a-egide-do-regulamento-europeu-de-protecao-de-dados--gdpr. Acesso em: 07 nov. 2020.

GDPR: Registro de multas aplicadas pela Lei Europeia de Proteção de Dados. In: **SegInfo**: portal, podcast e evento sobre segurança da informação. 30 mar. 2020. Disponível em: https://seginfo.com.br/2020/03/30/gdpr-registro-de-multas-aplicadas-pela-lei-europeia-de-protecao-de-dados/. Acesso em: 17 dez. 2020.

GOGONI, R. Temer sanciona, com vetos, a lei de proteção a dados pessoais; saiba o que muda e quando. In: **Meio bit**. 2018. Disponível em: https://tecnoblog.net/meiobit/389413/lei-protecao-dados-pessoais-sancionada-temer-com-vetos/. Acesso em: 12 dez. 2020.

GONÇALVES, F. R. Inversão do ônus da prova. In: Âmbito jurídico: o seu portal jurídico na internet. 01 fev. 2013. Disponível em: https://ambitojuridico.com.br/edicoes/revista-109/inversao-do-onus-da-prova/#:~:text=Como%20j%C3%A1%20explanado%2C%20a%20invers%C3%A3o,hipossuficiência%20e%20vulnerabilidade%20do%20consumidor. Acesso em: 25 jan. 2021.

GUALTIERI, G. As 10 bases legais para tratamento de dados permitidas pela LGPD. In: **Tripla**. 9 set. 2019. Disponível em: https://triplait.com/bases-legais-para-tratamento-de-dados-da-lgpd/. Acesso em: 15 nov. 2020.

GUIMARÃES, L. Qual a diferença entre dados informação? In: **Know Solutions**. [20--]. Disponível em: https://www.knowsolution.com.br/diferenca-dado-e-informacao/. Acesso em: 15 jun. 2020.

HIRATA, A. O Facebook e o direito à privacidade. **Revista de informação legislativa**, Brasília, v. 51, n. 201, p. 17-27, jan./mar. 2014. Disponível em: https://www2.senado.leg.br/bdsf/item/id/502950. Acesso em: 30 set. 2019.

KATHRIN. A GDPR completa 1 ano com bons resultados. In: **LeadComm**: performance and security. 30 jul. 2019. Disponível em: https://leadcomm.com.br/2019/07/30/a-gdpr-completa-1-ano-com-bons-resultados/#:~:text=A%20GDPR%20%C3%A9%20um%20regulamento,os%20seus%20casos%20de%20viola%C3%A7%C3%A3o. Acesso em: 15 nov. 2020.

Lei de Proteção de Dados Pessoal (PDPA) da Argentina. In: **Microsoft**. 02 dez. 2020. Disponível em: https://docs.microsoft.com/pt-br/compliance/regulatory/offering-pdpa-argentina. Acesso em: 21 dez. 2020.

LGPD e compliance: principais desafios e como vencê-los. In: **Ambra University**: Advocacia. 30 dez. 2019. Disponível em: https://www.direitoprofissional.com/lgpd-e-complice/. Acesso em: 04 jan. 2021.

LGPD: o que são dados pessoais sensíveis? In: **ConectaJá**: proteste. 20 ago. 2020. Disponível em: https://conectaja.proteste.org.br/lgpd-o-que-sao-dados-pessoais-sensiveis/. Acesso em: 27 dez. 2020.

MACÊDO, D. Ameaças comuns de engenharia social. In: **Diego Macêdo**: um pouco de tudo sobre T.I. 08 maio 2017. Disponível em: https://www.diegomacedo.com.br/tag/shoulder-surfing/#:~:text=No%20entanto%2C%20falando%20de%20engenharia,espionar%20a%20tela%20do%20outro. Acesso em: 17 nov. 2020.

Mineração de dados: o que é e qual sua importância?. In: **SAS**. [20--]. Disponível em: https://www.sas.com/pt_br/insights/analytics/mineracao-de-dados.html. Acesso em: 08 jun. 2020.

OLIVEIRA, A. P. de. *et al.* A lei geral de proteção de dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, Curitiba, v. 4, n. 1, maio, 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 24 jan. 2021.

Oversharing: entenda o que significa e sua relação com as emoções. In: **Sbie**. 22 set. 2016. Disponível em: https://www.sbie.com.br/blog/oversharing-entenda-o-que-significa-e-sua-relacao-com-as-emocoes. Acesso em: 12 dez. 2020.

Ônus da prova: novo CPC (Lei nº 13.105/15). In: **DireitoNet**, Dicionário jurídico. 04 jan. 2016. Disponível em: https://www.direitonet.com.br/dicionario/exibir/1560/Onus-da-prova-Novo-CPC-Lei-no-13105-15. Acesso em: 11 dez. 2020.

O que é NDA? Saia se sua empresa precisa de um. In: **BLB Brasil**: auditoria, consultoria e educação. 11 fev. 2019. Disponível em: https://www.blbbrasil.com.br/blog/nda/. Acesso em: 10 nov. 2020.

PARASCHIV, P. GDPR for libraries: identifying the personal data you are processing [data map template]. In: **Princh**. Aarhus, Denmark, 6 abr. 2018. Disponível em: https://princ.com/gdpr-for-libraries-identifying-the-personal-data/#.YBNTTzEzbIU. Acesso em: 28 jan. 2021.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

PEIXOTO, A. S. Lei de Proteção de dados: entenda em 13 pontos! In: **Politize!** 14 jan. 2020. Disponível em: https://www.politize.com.br/lei-de-protecao-de-dados/. Acesso em: 16 ago. 2020.

Privacidade de dados no Japão. In: **AWS**. [20--]. Disponível em: https://aws.amazon.com/pt/compliance/japan-data-privacy/. Acesso em: 20 dez. 2020.

Proteção de dados: entenda mais sobre o assunto! In: **Impacta**. 02 set. 2019. Disponível em: https://www.impacta.com.br/blog/protecao-de-dados-entenda-mais-sobre-o-assunto/. Acesso em: 30 set. 2020.

Quais os impactos da LGPD no Brasil? In: **InContract**. [20--]. Disponível em: https://www.incontract.com.br/lgpd/. Acesso em: 03 jan. 2021.

Quais são os países com maior proteção de dados pessoais. In: **Privacytools**. [20--]. Disponível em: https://privacytools.com.br/quais-sao-os-paises-com-maior-protecao-de-dados-pessoais. Acesso em: 07 jan. 2021.

Quem vai regular a LGPD?. In: **Serpro e LGPD**: segurança e inovação. [20--]. Disponível em: https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd#:~:text=A%20ANPD%2C%20que%20est%C3%A1%20em,Dados%20Pessoais%20e%20da%20Privacidade. Acesso em: 12 dez. 2020.

RAMOS, P. H. O otimismo com a LGPD pode ser ilusório. Entenda por que a nova lei de proteção de dados já começa cercada de incertezas. In: **Draft**. 16 set. 2020. Disponível em: https://www.projetodraft.com/por-que-a-lgpd-ja-comeca-cercada-de-incertezas/. Acesso em: 06 nov. 2020.

ROCHA, M. O. Mercado de trabalho na era da informática. In: **Direitonet.** 09 dez. 2005, Direito trabalhista. Disponível em: https://www.direitonet.com.br/artigos/exibir/2361/Mercado-de-trabalho-na-era-da-informatica. Acesso em: 23 jan. 2021.

ROCHER, L. *et al.* Estimating the success of re-identifications inincomplete datasets using generative models. **Nature Communications**, v. 10, p. 1–9, 2019. Disponível em: https://doi.org/10.1038/s41467-019-10933-3. Acesso em: 12 mar. 2021.

SANTOS. I. M. O que fazer em caso de vazamento de dados? In: **Federasul**. 29 nov. 2019. Disponível em: https://www.federasul.com.br/o-que-fazer-em-caso-de-vazamento-de-dados/. Acesso em: 20 dez. 2020.

SOARES, P. S. C. Legítimo interesse como hipótese para tratamento de dados. In: **Consultor jurídico**. 18 jun. 2019. Disponível em: https://www.conjur.com.br/2019-jun-18/pedro-soares-tratamento-dados-baseado-legitimo-interesse. Acesso em: 21 nov. 2020.

STAUDT, M. Vida de instagram: a síndrome da vida perfeita. In: **New order**. 29 jul. 2017. Disponível em: https://medium.com/neworder/vida-de-instagram-a-s%C3%ADndrome-da-vida-perfeita-2d2a0bcbe372. Acesso em: 14 dez. 2020.

TEIXEIRA FILHO, J. **Gerenciando conhecimento**: como a empresa pode usar a memória organizacional e a inteligência competitiva no desenvolvimento de negócios. Rio de Janeiro: Ed. SENAC, 2000.

TIEGHI, A. L. Empresas buscam se adaptar à Lei Geral de Proteção de Dados: multas começam só em 2021, mas contratos já exigem adequação às normas. In: **Folha de São Paulo**. São Paulo, 19 out. 2020. Disponível em: https://www1.folha.uol.com.br/mpme/2020/10/empresas-buscam-se-adaptar-a-lei-que-protege-dados-de-clientes.shtml. Acesso em: 19 dez. 2020.

Tudo sobre phishing. In: **Malwarebytes**. [20--]. Disponível em: https://br.malwarebytes.com/phishing/#:~:text=Phishing%20%C3%A9%20o%20crime%20de,phishing%20%C3%A9%20a%20mais%20comum.. Acesso em: 19 nov. 2020.

URUPÁ, Marcos. Lei de privacidade da Califórnia começa a valer e é a mais abrangente dos EUA. In: **Teletime**. 13 jan. 2020. Disponível em: https://teletime.com.br/13/01/2020/lei-de-privacidade-da-california-comeca-a-valer-e-e-a-mais-abrangente-dos-eua/. Acesso em: 07 jan. 2021.

VALENTE, J. Legislação de proteção de dados já é realidade em outros países. In: **Agência Brasil**. Brasília, 07 maio 2018. Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2018-05/legislacao-de-protecao-de-dados-ja-e-realidade-em-outros-paises. Acesso em: 20 dez. 2020.

VIEIRA, I. Como funcionam os algoritmos das redes sociais. In: **Blog de Marketing Digital de Resultados**. 11 set. 2020. Disponível em: https://resultadosdigitais.com.br/blog/algoritmo-facebook-instagram-twitter/. Acesso em: 15 nov. 2020.

ZEFERINO, D. Proteção de dados: como adequar a sua empresa à LGPD? In: **Certifiquei**: segurança da informação. 29 jul. 2020. Disponível em: https://www.certifiquei.com.br/protecao-dados/. Acesso em: 20 nov. 2020.

APÊNDICE A – Formulário de Pesquisa

Questões	**Respostas**
Idade:	Campo aberto
Cidade e Estado	Campo aberto
Profissão	Campo aberto
Nível de escolaridade	Ensino fundamental incompleto Ensino fundamental completo Ensino médio incompleto Ensino médio completo Ensino superior completo (ou graduação) Pós-graduação Mestrado/Doutorado/Pós-Doutorado
1) Você sabe o que é proteção de dados pessoais?	Sim/Não
2) Você sabe o que é LGPD?	Sim/Não
3) Você lê os termos de adesão ou política de privacidade dos serviços que costuma contratar?	Sim/Não
4) Na sua opinião, seus dados pessoais estão protegidos?	Sim/Não
5) Para qualquer tipo de aquisição ou utilização de serviços é necessário informar dados pessoais. Você conhece a finalidade de utilização de seus dados para esses serviços contratados?	Sim/Não
6) Na sua opinião, seus dados pessoais e interesses são importantes para uma organização/empresa?	Sim/Não

APÊNDICE B – Questionário enviado aos especialistas

1) Ao seu entender, a LGPD se aplica aos indivíduos que desconhecem o seu dado como um direito individual? Por exemplo, um indivíduo que desconhece da LGPD e aceita todos os termos de condições e todas as políticas de privacidade.	Resposta livre
2) Conforme artigo da constituição, que prevê a privacidade como um direito, é possível alcançar a privacidade com a LGPD?	Resposta livre
3) Em sua opinião, nossos dados estão protegidos?	Resposta livre
4) Qual o real motivo da criação da LGPD?	Resposta livre
5) Quais as falhas existentes na LGPD ao seu entender?	Resposta livre
6) Legítimo interesse pode ser utilizado em que situação?	Resposta livre
7) Como ficam os dados de menores de 18 anos, caso o responsável não de consentimento, em bases legais como: interesse vital ou tutela da saúde?	Resposta livre
8) A ANPD funcionará como a ANATEL e receberá reclamações? Todas serão analisadas?	Resposta livre
9) Como uma pessoa pode ter proteção de dados sem conhecer a LGPD?	Resposta livre

ANEXOS A - Lei geral de proteção de dados

Presidência da República

Secretaria-Geral

Subchefia para Assuntos Jurídicos

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.

Texto compilado

Mensagem de veto

Vigência

~~Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).~~

Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) Vigência

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei 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.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 2º A disciplina da proteção de dados pessoais tem como 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.

Art. 3º 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;~~
~~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 (Redação dada pela Medida Provisória nº 869, de 2018)~~

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 (Redação dada pela Lei nº 13.853, de 2019) Vigência

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.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;~~
~~b) acadêmicos; (Redação dada pela Medida Provisória nº 869, de 2018)~~

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - 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; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência

internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

~~§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.~~

~~§ 2º O tratamento dos dados a que se refere o inciso III do **caput** por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público, hipótese na qual será observada a limitação de que trata o § 3º.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

~~§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.~~

~~§ 3º Os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do **caput** não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

~~§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado.~~ ~~(Revogado pela Medida Provisória nº 869, de 2018)~~

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

~~VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;~~

~~VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - agentes de tratamento: o controlador e o operador;

X - 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;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;~~

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Medida Provisória nº 869, de 2018)~~

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

~~XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.~~

~~XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. (Redação dada pela Medida Provisória nº 869, de 2018)~~

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

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

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

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

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

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

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

~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~

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

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

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

~~§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

~~§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 8º 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.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II
Do Tratamento de Dados Pessoais Sensíveis

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

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

~~f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou~~

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

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.~~

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de: (Redação dada pela Medida Provisória nº 869, de 2018)~~

~~I - portabilidade de dados quando consentido pelo titular; ou (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar. (Incluído pela Medida Provisória nº 869, de 2018)~~

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares

de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) Vigência

I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) Vigência

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

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

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III
Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV
Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

~~V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;~~

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

~~Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~

~~Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I
Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - (VETADO); e

~~III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.~~

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal , terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) ;

II - (VETADO);

~~III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~

~~III - se for indicado um encarregado para as operações de tratamento de dados pessoais, nos termos do art. 39;~~ ~~Redação dada pela Medida Provisória nº 869, de 2018)~~

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

~~IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

~~V - na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019) Vigência

~~VI - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)~~

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:~~

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá de consentimento do titular, exceto: (Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 28. (VETADO).

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público a realização de operações de tratamento de dados pessoais, as informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II
Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V
DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI
DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Seção III
Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

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 mencionar, 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 para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II
Das Boas Práticas e da Governança

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.

§ 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.

§ 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:

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;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Das Sanções Administrativas

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;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

~~X - (VETADO); (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

~~XI - (VETADO); (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

~~XII - (VETADO). (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

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 nº 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 nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

§ 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:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

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; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

~~§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.~~

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019) Vigência

~~§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .~~

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011. (Redação dada pela Lei nº 13.853, de 2019)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. (Incluído pela Lei nº 13.853, de 2019)

~~§ 6º (VETADO). (Incluído pela Lei nº 13.853, de 2019)~~ (Promulgação partes vetadas)

§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas: (Incluído pela Lei nº 13.853, de 2019)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e (Incluído pela Lei nº 13.853, de 2019)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. (Incluído pela Lei nº 13.853, de 2019)

§ 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. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (Vigência)

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. (Vigência)

CAPÍTULO IX
DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I
Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. (VETADO).

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-B. É assegurada autonomia técnica à ANPD. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-C. ANPD é composta por: (Incluído pela Medida Provisória nº 869, de 2018)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Medida Provisória nº 869, de 2018)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Medida Provisória nº 869, de 2018)

III - Corregedoria; (Incluído pela Medida Provisória nº 869, de 2018)

IV - Ouvidoria; (Incluído pela Medida Provisória nº 869, de 2018)

V - órgão de assessoramento jurídico próprio; e (Incluído pela Medida Provisória nº 869, de 2018)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei." (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-D. O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente. (Incluído pela Medida Provisória nº 869, de 2018)

§ 1º Os membros do Conselho Diretor da ANPD serão nomeados pelo Presidente da República e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superior - DAS de nível 5. (Incluído pela Medida Provisória nº 869, de 2018)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Medida Provisória nº 869, de 2018)

§ 3º O mandato dos membros do Conselho Diretor será de quatro anos. (Incluído pela Medida Provisória nº 869, de 2018)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de dois, de três, de quatro, de cinco e de seis anos, conforme estabelecido no ato de nomeação. (Incluído pela Medida Provisória nº 869, de 2018)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Medida Provisória nº 869, de 2018)

§ 1º Nos termos do **caput** , cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Medida Provisória nº 869, de 2018)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, caso necessário, e proferir o julgamento. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013 . (Incluído pela Medida Provisória nº 869, de 2018)

Parágrafo único. A infração ao disposto no **caput** caracteriza ato de improbidade administrativa. (Incluído pela Medida Provisória nº 869, de 2018)

Art.55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Medida Provisória nº 869, de 2018)

Parágrafo único. Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Medida Provisória nº 869, de 2018)

Art. 55-J. Compete à ANPD: (Incluído pela Medida Provisória nº 869, de 2018)

I - zelar pela proteção dos dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)

II - editar normas e procedimentos sobre a proteção de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)

III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos; (Incluído pela Medida Provisória nº 869, de 2018)

IV - requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)

V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; (Incluído pela Medida Provisória nº 869, de 2018)

VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Medida Provisória nº 869, de 2018)

VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Medida Provisória nº 869, de 2018)

~~VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~XVI - elaborar relatórios de gestão anuais acerca de suas atividades. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 1º A ANPD, na edição de suas normas, deverá observar a exigência de mínima intervenção, assegurados os fundamentos e os princípios previstos nesta Lei e o disposto no art. 170 da Constituição. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 2º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 3º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 4º No exercício das competências de que trata o **caput** , a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 5º As reclamações colhidas conforme o disposto no inciso V do **caput** poderão ser analisadas de forma agregada e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, cujas demais competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Parágrafo único. A ANPD articulará sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019)

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V - órgão de assessoramento jurídico próprio; e (Incluído pela Lei nº 13.853, de 2019)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019)

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019)

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019)

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019)

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019)

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019)

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019)

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019)

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019)

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019)

XII - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019)

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019)

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019)

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019)

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019)

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019)

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. (Incluído pela Lei nº 13.853, de 2019)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. (Incluído pela Lei nº 13.853, de 2019)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. (Incluído pela Lei nº 13.853, de 2019)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

Art. 55-L. Constituem receitas da ANPD: (Incluído pela Lei nº 13.853, de 2019)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; (Incluído pela Lei nº 13.853, de 2019)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; (Incluído pela Lei nº 13.853, de 2019)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; (Incluído pela Lei nº 13.853, de 2019)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; (Incluído pela Lei nº 13.853, de 2019)

V - (VETADO); (Incluído pela Lei nº 13.853, de 2019)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; (Incluído pela Lei nº 13.853, de 2019)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. (Incluído pela Lei nº 13.853, de 2019)

Art. 56. (VETADO).

Art. 5 7. (VETADO).

Seção II
Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

~~Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes, titulares suplentes, dos seguintes órgãos: (Incluído pela Medida Provisória nº 869, de 2018)~~

~~I - seis do Poder Executivo federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - um do Senado Federal; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~III - um da Câmara dos Deputados; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IV - um do Conselho Nacional de Justiça; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V - um do Conselho Nacional do Ministério Público; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VI - um do Comitê Gestor da Internet no Brasil; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VII - quatro de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~VIII - quatro de instituições científicas, tecnológicas e de inovação; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IX - quatro de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 1º Os representantes serão designados pelo Presidente da República. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 2º Os representantes de que tratam os incisos I a VI do **caput** e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 3º Os representantes de que tratam os incisos VII, VIII e IX do **caput** e seus suplentes: (Incluído pela Medida Provisória nº 869, de 2018)~~

~~I - serão indicados na forma de regulamento; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - terão mandato de dois anos, permitida uma recondução; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~III - não poderão ser membros do Comitê Gestor da Internet no Brasil. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Medida Provisória nº 869, de 2018)~~

~~I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: (Incluído pela Lei nº 13.853, de 2019)

I - 5 (cinco) do Poder Executivo federal; (Incluído pela Lei nº 13.853, de 2019)

II - 1 (um) do Senado Federal; (Incluído pela Lei nº 13.853, de 2019)

III - 1 (um) da Câmara dos Deputados; (Incluído pela Lei nº 13.853, de 2019)

IV - 1 (um) do Conselho Nacional de Justiça; (Incluído pela Lei nº 13.853, de 2019)

V - 1 (um) do Conselho Nacional do Ministério Público; (Incluído pela Lei nº 13.853, de 2019)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; (Incluído pela Lei nº 13.853, de 2019)

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; (Incluído pela Lei nº 13.853, de 2019)

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; (Incluído pela Lei nº 13.853, de 2019)

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e (Incluído pela Lei nº 13.853, de 2019)

XI - 2 (dois) de entidades representativas do setor laboral. (Incluído pela Lei nº 13.853, de 2019)

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública. (Incluído pela Lei nº 13.853, de 2019)

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes: (Incluído pela Lei nº 13.853, de 2019)

I - serão indicados na forma de regulamento; (Incluído pela Lei nº 13.853, de 2019)

II - não poderão ser membros do Comitê Gestor da Internet no Brasil; (Incluído pela Lei nº 13.853, de 2019)

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução. (Incluído pela Lei nº 13.853, de 2019)

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada. (Incluído pela Lei nº 13.853, de 2019)

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. (Incluído pela Lei nº 13.853, de 2019)

Art. 59. (VETADO).

CAPÍTULO X
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) , passa a vigorar com as seguintes alterações: Vigência

"Art. 7º .....

.....

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

....." (NR)

"Art. 16. .....

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

~~Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 . (Revogado pela Medida Provisória nº 869, de 2018)~~

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

~~Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial .~~

~~Art. 65. Esta Lei entra em vigor:~~ ~~(Redação dada pela Medida Provisória nº 869, de 2018)~~

~~I - quanto aos art. 55-A, art. 55-B, art. 55-C, art. 55-D, art. 55-E, art. 55-F, art. 55-G, art. 55-H, art. 55-I, art. 55-J, art. 55-K, art. 58-A e art. 58-B, no dia 28 de dezembro de 2018; e~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - vinte e quatro meses após a data de sua publicação quanto aos demais artigos.~~ ~~(Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

~~II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.~~ ~~(Incluído pela Lei nº 13.853, de 2019)~~

~~II - em 3 de maio de 2021, quanto aos demais artigos.~~ ~~(Redação dada pela Medida Provisória nº 959, de 2020)~~ (Convertida na Lei nº 14.058, de 2020)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília , 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Torquato Jardim

Aloysio Nunes Ferreira Filho

Eduardo Refinetti Guardia

Esteves Pedro Colnago Junior

Gilberto Magalhães Occhi

Gilberto Kassab

Wagner de Campos Rosário

Gustavo do Vale Rocha

Ilan Goldfajn

Raul Jungmann

Eliseu Padilha

Este texto não substitui o publicado no DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra

*

GLOSSÁRIO

AIPD - Avaliação de impacto sobre a proteção de dados.

GDPR – *General Data Protection Regulation* – Regulamento Geral de Proteção de Dados – Regras de privacidade da União Europeia.

IP – Número exclusivo de protocolo de internet.

LGPD – Lei geral de proteção de dados Brasil;

LDPA ou PDPS -*Ley de Protección de los Datos Personales* – Lei de Proteção de dados pessoais da Argentina.

UE – União Europeia.