Universidade de Brasília - UnB

Faculdade de Direito

Curso de Graduação em Direito

NICOLE MACHADO DA SILVA CREMONEZ

O USO DE DADOS PESSOAIS DE TRABALHADORES OBTIDOS EM INVESTIGAÇÕES INTERNAS PARA A CELEBRAÇÃO DE ACORDOS DE COOPERAÇÃO COM A ADMINISTRAÇÃO PÚBLICA:

Como se adequar ao dever de estar em conformidade com a LGPD?

Brasília, 2021.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

Nicole Machado da Silva Cremonez

O USO DE DADOS PESSOAIS DE TRABALHADORES OBTIDOS EM INVESTIGAÇÕES INTERNAS PARA A CELEBRAÇÃO DE ACORDOS DE COOPERAÇÃO COM A ADMINISTRAÇÃO PÚBLICA:

Como se adequar ao dever de estar em conformidade com a LGPD?

Monografia apresentada como requisito parcial à obtenção do grau de Bacharela em Direito pela Faculdade de Direito da Universidade de Brasília - UnB.
Orientadora: Profa. Dra. Amanda Athayde Linhares Martins Rivera.

Brasília, 2021.

TERMO DE APROVAÇÃO

Nicole Machado da Silva Cremonez

O USO DE DADOS PESSOAIS DE TRABALHADORES OBTIDOS EM INVESTIGAÇÕES INTERNAS PARA A CELEBRAÇÃO DE ACORDOS DE COOPERAÇÃO COM A ADMINISTRAÇÃO PÚBLICA: Como adequar ao dever de estar em conformidade com a LGPD?

Monografia apresentada como requisito parcial à obtenção do grau de Bacharela em Direito pela Faculdade de Direito da Universidade de Brasília - UnB.
Orientadora: Profa. Dra. Amanda Athayde Linhares Martins Rivera.
Brasília, 20 de maio de 2021.

_____

Professora Dra. Amanda Athayde Linhares Martins Rivera,
Doutora em Direito pela Universidade de São Paulo
Professora Orientadora

_____

Professora Dra. Ana de Oliveira Frazão,
Integrante da banca examinadora

_____

Professora Mônica Tiemy Fujimoto,
Integrante da banca examinadora

AGRADECIMENTOS

Este trabalho representa o encerramento de um ciclo e o início de novos desafios. Muito além dos aprendizados acadêmicos e técnicos, levarei comigo experiências e, principalmente, amizades para toda a vida. Por isso, apresento meus agradecimentos às pessoas que fizeram parte dessa trajetória.

Agradeço à Professora Amanda Athayde Linhares Martins Rivera por rapidamente aceitar me orientar neste trabalho e fazer dele um resultado muito melhor do que eu imaginava. Agradeço também aos demais membros da banca, professoras Ana de Oliveira Frazão e Mônica Tiemy Fujimoto - cujos conhecimentos e pensamentos foram muito valiosos na concepção deste trabalho, por aceitarem o meu convite.

À minha família, nada disso teria sido possível sem vocês. Aos meus avós, Lucio, Celia e Cléa, gratidão eterna por terem me permitido chegar até aqui e por toda vida terem sido apoiadores e torcedores sem igual. Às minhas bisas Celeste e Helena, e ao meu avô Sebastião, posso sentir a torcida e celebração nas minhas vitórias aí de cima. Ainda lhes proporcionarei muitas alegrias.

Aos meus pais, que sempre incentivaram e possibilitaram os meus estudos, por muitas vezes renunciando a outras coisas para isso. Eu reconheço o empenho de vocês. À minha mãe, Ana Cristina, que sempre me apoiou, a seu modo, e se desdobrou para que eu concretizasse meus desejos e sonhos. Um modelo de resiliência, humildade e devoção.

Ao meu pai, Robson, inspiração de disciplina, foco e disposição. Foram suas cobranças e o alto nível de exigência que me instigam a querer crescer e melhorar cada vez mais. À minha irmã, Natália, a caminhada ficou mais leve e divertida na sua companhia.

Aos meus tios, Cláudio, Suzana, Cristina e Fábio, por todos os abraços amorosos – ainda que poucos devido à distância. Aos meus primos, Lucas, André e Hugo, pela alegria e parceria quando juntos.

Ao Vitor, que esteve ao meu lado nessa jornada, meu muito obrigada por compartilhar as mais diversas experiências. Exemplo de esforço e dedicação, você é uma inspiração. Gratidão por acreditar em mim e me incentivar a alcançar meus sonhos. Vivenciá-los com você é fantástico.

Aos amigos da UnB, a convivência e amizade de todos tornou tudo mais prazeroso. Ganhei amigos para a vida. Meu agradecimento especial a alguns deles: Aline Cristina Pereira da Silva, Luís Carlos Moura Guimarães, Maiara Cristina Schiavom da Silva, Mariana Barreto

Ribeiro e Marina Ratti de Andrade. Aos demais colegas de UnB, agradeço pelas risadas e experiências proporcionadas. Gratidão também a amigos que fizeram parte dessa jornada, ainda que fora da UnB, em especial a Aline da Silva Barros, Bárbara Esteves, Lucas Pessoa de Lima, Maria Clara Durão, Raquel da Gama Pinheiro e Sandra Barbosa Pereira.

Por fim, agradeço aos demais professores e profissionais que participaram da minha formação, bem como aos inúmeros projetos que a universidade me proporcionou, em especial ao Veredicto, por tantas experiências e aprendizados. Não poderia, também, deixar de agradecer à Universidade de Brasília por abrir a minha cabeça e me mostrar que a diversidade e a diferença de opiniões são necessárias na construção de um mundo melhor. Terei orgulho de ter passado por esta instituição.

Resumo

O presente trabalho possui como tema a possibilidade de uso de dados pessoais colhidos pelas investigações internas no âmbito dos programas de *compliance* das empresas para celebração de acordos de cooperação com a administração pública. Dentre os objetivos desta pesquisa, vale dizer que, em seu sentido mais amplo, é analisar os requisitos definidos pela LGPD para que a empresa possa utilizar dados de trabalhadores obtidos em investigações internas de *compliance* para a celebração de acordos com a administração pública. Nomeadamente, pretende-se, também, identificar potencial choque entre o direito à privacidade de dados e o interesse legítimo das empresas, mapear os limites de natureza, coleta, uso, tratamento, armazenamento e eliminação de dados pessoais definidos na LGPD e elencar os requisitos necessários para uso de dados pessoais oriundos de investigações internas nos acordos com a administração pública. Pretende-se - por meio de pesquisa exploratória qualitativa e análises bibliográficas - demonstrar que, a fim de que esses direitos sejam harmonizados, deve-se observar os requisitos e limites contidos na LGPD relativos à natureza, coleta, tratamento, uso, armazenamento e eliminação de dados pessoais para que sejam utilizados como prova da conduta na celebração de acordos com a administração pública.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD). *Compliance*. Investigações internas. Acordos de cooperação. Dados pessoais.

Abstract

The present work has as its theme the possibility of using personal data collected by internal investigations within the scope of companies' compliance programs to conclude cooperation agreements with the public administration. Among the objectives of this research, it is worth mentioning that, in its broadest sense, it is the analysis of the requirements defined by the LGPD so that the company can use data from workers allowed in internal compliance investigations to conclude agreements with the public administration. In particular, it is also intended to identify the potential clash between the right to data privacy and the legitimate interest of companies, to map the limits of nature, collection, use, treatment, storage and disposal of personal data defined in the LGPD and to list the requirements mandatory for the use of personal data from internal investigations in agreements with the public administration. It is intended - through qualitative exploratory research and bibliographic analysis - to demonstrate that, in order for these rights to be harmonized, one must observe the requirements and limits contained in the LGPD regarding the nature, collection, treatment, use, storage and disposal personal data to be used as evidence of conduct in entering into agreements with the public administration.

Keywords: General Data Protection Act (LGPD). Compliance. Internal investigations. Cooperation agreements. Personal data.

SUMÁRIO

Lista de siglas

ANPD: Autoridade Nacional de Proteção de Dados

Bacen: Banco Central do Brasil

Cade: Conselho Administrativo de Defesa Econômica

CC: Código Civil

CDC: Código de Defesa do Consumidor

CF: Constituição Federal

CNH: Carteira Nacional de Habilitação

CPC: Código de Processo Civil

CPF: Cadastro de Pessoa Física

CTPol: centro de Estudos em Comunicação, Política e Tecnologia

CVM: Comissão de Valores Mobiliários

DPO: *Data Protection Officer*

IBGC: Instituto Brasileiro de Governança Corporativa

IP: *Internet Protocol*

GPS: *Global Positioning System*

LIA: *legitimate interest assessment*

LGPD: Lei Geral de Proteção de Dados Pessoais

MP: Ministério Público

MPF: Ministério Público Federal

GDPR: Regulamento Geral de Proteção de Dados da União Europeia

RICade: Regimento Interno do Cade

RG: Registro Geral

RH: Recursos Humanos

TI: Tecnologia da Informação

TIC: Tecnologias da Informação e da Comunicação

TCC: Termo de Compromisso de Cessação

TJRS: Tribunal de Justiça do Rio Grande do Sul

1 INTRODUÇÃO

O presente trabalho possui como tema a possibilidade de uso de dados pessoais colhidos pelas investigações internas no âmbito dos programas de *compliance* das empresas para celebração de acordos de cooperação com a administração pública.

Devido ao avanço tecnológico decorrente da globalização, que guia os negócios da atual economia digital, as informações pessoais tornaram-se elementos cruciais[1]. Essas informações são coletadas, processadas e utilizadas em diversos canais e plataformas de maneiras nunca imaginadas, como por exemplo: conteúdos pesquisados pelo usuário que se tornam anúncios em plataformas digitais, uso do áudio dos celulares para sugestão de anúncios, uso da localização para sugestão de rotas, entre outros.

Com o alto grau de compartilhamento e processamento de dados, havia um desequilíbrio ante o direito de proteção de dados e o direito de proteção da privacidade e intimidade das pessoas[2]. Em contrapartida, estava sendo privilegiado o interesse das empresas em processar dados de usuários para fins comerciais. Por conseguinte, viu-se a necessidade de criar normas para a proteção de dados pessoais[3].

Manuel Castells[4] define a atual sociedade em rede como "uma sociedade cuja estrutura social é construída em torno de redes ativadas por tecnologias de comunicação e de informação processadas digitalmente e baseadas na microeletrônica". Um ponto relevante é que a sociedade em rede ao mesmo tempo que amplifica o poder de comunicação entre os indivíduos, amplia, também, o seu potencial lesivo.

Na Europa, a aprovação de instrumento normativo que disciplina o direito à privacidade se deu anos atrás, com o Regulamento Geral de Proteção de Dados (GDPR), que versa sobre a proteção de dados pessoais de pessoas físicas e a forma de se operar com essas informações. Diante disso, foi exigido que os países que possuíam relações comerciais com a Europa criassem normas equivalentes para que não fossem impostas maiores dificuldades aos negócios[5]. Dentre outros motivos, isso estimulou a criação da LGPD no Brasil.

---

[1] PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018, p. 17.
[2] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 24.
[3] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: A função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019, p. 4.
[4] CASTELLS, Manuel. O Poder da Comunicação. São Paulo: Paz e Terra, 2015.
[5] PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018, p. 18.

O Brasil passou a sofrer grande influência para se adequar ao Regulamento Geral de Proteção de Dados da União Europeia após a implantação, já que a norma não atingia somente as empresas europeias, mas também as empresas contratadas por estas que não possuíssem nível de proteção de dados compatíveis[6]. Houve, também, incidentes relacionados a operações indevidas com dados pessoais e vazamentos. Sendo assim, foi percebida a necessidade da regulamentação da operação desses dados, e, consequentemente, surgiram projetos visando a proteção de dados pessoais no Brasil.

A Lei Geral de Proteção de Dados Pessoais, Lei 13.709 de 14 de agosto de 2018, conhecida como LGPD, tenciona regular o tratamento de dados pessoais por pessoa jurídica, de direito público ou privado, seja no meio físico ou no digital, de todas as pessoas envolvidas[7]. Isto posto, essa lei se aplica a todas as empresas e a administração pública, não obstante algumas exceções previstas em seu artigo 4º, como no caso de tratamento de dados pessoais realizado por pessoa natural, desde que exclusivamente para fins particulares e/ou não econômicos, ou, ainda, para fins artísticos, acadêmicos ou de segurança nacional[8].

A LGPD objetiva "[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[9]. Em outras palavras, almeja "[...] resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa"[10]. Vale citar que, conforme a LGPD, tratamento de dados é "[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção recepção, classificação, acesso, [...] armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"[11].

---

[6] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 23.

[7] BRASIL. Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 10 maio 2020; BLUM, Rita Peixoto Ferreira; MORAES, Helio Ferreira. Lei Geral de Proteção de Dados Pessoais - LGPD. In: CARVALHO, André Castro et. al. Manual de Compliance. 2. ed. Rio de Janeiro: Forense, 2020. p. 502.

[8] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 dezembro 2020.

[9] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 dezembro 2020.

[10] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 100.

[11] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 dezembro 2020.

Na mesma proporção, são considerados dados pessoais para fins de tratamento aqueles relacionados a qualquer informação de pessoa natural identificada ou identificável, inclusive de acesso público, como também informações extremamente particulares, os chamados dados sensíveis[12], que podem levar uma pessoa a sofrer discriminação. Se descumpridos os requisitos legais, poderá haver aplicação de sanções administrativas, desde advertência até a imputação de multa[13]. Sendo assim, percebe-se os possíveis impactos e a importância da implementação de boas práticas de governança corporativa, mais especificamente, de mecanismos de *compliance*, nas instituições. Dessa forma, é possível prevenir infrações ou reduzir seus impactos.

Por sua vez, o *compliance* é tido como um mecanismo de autorregulação baseado na criação de sistemas internos à pessoa jurídica que se direcionam a assegurar o cumprimento, a conformidade e a execução da lei[14]. Para isso, busca "estabelecer mecanismos e procedimentos que tornem o cumprimento da legislação parte da cultura corporativa[15]. No entanto, não busca "eliminar completamente a chance de ocorrência de um ilícito, mas sim minimizar as possibilidades de que ele ocorra, e criar ferramentas para que a empresa rapidamente identifique sua ocorrência e lide da forma mais adequada possível com o problema"[16].

Percebida a conduta ilícita praticada por funcionário da empresa, seja por meio de denúncia ou de auditoria, cabe à empresa tomar as devidas precauções para que não sejam cometidos mais atos do tipo, as medidas necessárias para seu reparo e, ainda, promover denúncia à autoridade competente pela fiscalização. Nessa oportunidade, há a possibilidade de ser realizado acordo de cooperação entre a empresa e a administração pública, que pode proporcionar inúmeros benefícios para ambas, desde que cumpridos alguns requisitos.

No que tange aos acordos de cooperação, concebe-se por Acordo de Leniência aquele celebrado entre uma autoridade pública investigadora e um agente privado, seja pessoa física ou jurídica, com o fim de que a autoridade conceda a extinção ou abrandamento da penalidade aplicável ao agente, recebendo, em troca, provas e colaboração material e processual para que

---

[12] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 dezembro 2020.

[13] PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018, p. 109.

[14] RIBEIRO, Márcio de Aguiar. Responsabilização administrativa de pessoas jurídicas à luz da Lei Anticorrupção Empresarial. Belo Horizonte: Fórum. 2017. Fls. 201 e 202.

[15] Mendes, Francisco Schertel. Compliance: conconrrência e combate à corrupção. São Paulo: Trevisan Editora. 2017. Fl. 31.

[16] Mendes, Francisco Schertel. Compliance: conconrrência e combate à corrupção. São Paulo: Trevisan Editora. 2017. Fl. 31.

seja realizada a investigação[17]. Há, também, os programas de leniência, que são um arcabouço jurídico que dispõem de incentivos por parte da autoridade pública investigadora para que os agentes privados tomem iniciativa de a procurar para negociar sobre os referidos acordos[18].

Por sua vez, as medidas adotadas nas investigações internas relacionadas à celebração de acordos com a administração pública envolvem acesso a equipamentos eletrônicos, documentos, e-mails, redes sociais, localização e todo e qualquer dado que esteja ao alcance dos investigadores, que serão compartilhados após o tratamento com o poder público. Não seria essa uma violação aos direitos de privacidade dos executivos, dos funcionários e até mesmo de terceiros? Fato é que a LGPD introduziu no ordenamento jurídico brasileiro a necessidade de tratamento adequado desses dados pessoais[19].

Nesse sentido, surge a pergunta de pesquisa que se visa a responder com o presente trabalho: quais os requisitos definidos pela LGPD para que a empresa possa utilizar dados de trabalhadores obtidos em investigações internas de *compliance* para a celebração de acordos com a administração pública quando tal trabalhador não é colaborador do acordo? Ao final do estudo, conforme será visto, conclui-se que, para isso, devem ser preenchidos os requisitos da base legal do legítimo interesse.

Frente ao avanço da tecnologia e, consequentemente, da modernidade dos meios de comunicação, a informação passou a dispor de grande importância, pois se tornou o elemento central para o desenvolvimento da economia. No que tange às empresas, é enorme o volume e variedade de informações que a permeiam. As organizações passaram a utilizar toda e qualquer informação que estivesse às suas mãos, sendo muitas de caráter pessoal, até o advento da LGPD.

Sabe-se que há requisitos na lei que devem ser observados para lidar com dados pessoais, seja para tratar, armazenar ou descartar. Entretanto, mesmo que as empresas cumpram com o descrito na LGPD, ainda há uma lacuna a ser discutida: os dados pessoais coletados pelas empresas, seja rotineiramente ou por meio de investigações internas realizadas por seus programas de *compliance*, podem ser utilizados para atender ao interesse dela quando da celebração de acordos de cooperação com a administração pública? Será evidenciado que sim, desde que preenchidos os requisitos da base legal do legítimo interesse.

---

[17] ATHAYDE, Amanda. **Manual dos Acordos de Leniência no Brasil:** teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 25.

[18] ATHAYDE, Amanda. **Manual dos Acordos de Leniência no Brasil:** teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 25.

[19] Segundo a LGPD (artigo 5º, I), dado pessoal é e qualquer informação que identifique ou que possa identificar uma pessoa física, de acordo com a concepção expansionista.

Há um potencial choque de direitos nessa situação, visto que, por um lado, deve ser observado o direito à privacidade das pessoas e, por outro, os interesses legítimos da empresa, ou o cumprimento de obrigação legal ou regulatória. Nessa perspectiva, esta pesquisa justifica-se em razão da atualidade do tema, já que todos terão que se adaptar às mudanças decorrentes da nova legislação, apesar de seus impactos só começarem a ser percebidos mais à frente. Ademais, servirá como apoio aos operadores do direito no que tange a quais requisitos devem ser observados para obter os efeitos tencionados na legislação de proteção de dados pessoais com o intuito de evitar violações futuras.

Dentre os objetivos desta pesquisa, vale dizer que, em seu sentido mais amplo, é analisar os requisitos definidos pela LGPD para que a empresa possa utilizar dados de trabalhadores obtidos em investigações internas de *compliance* para a celebração de acordos com a administração pública. Nomeadamente, pretende-se, também: *(i)* identificar potencial choque entre o direito à privacidade de dados e o interesse legítimo das empresas; *(ii)* mapear os limites de natureza, coleta, uso, tratamento, armazenamento e eliminação de dados pessoais definidos na LGPD; e *(iii)* elencar os requisitos necessários para uso de dados pessoais oriundos de investigações internas nos acordos com a administração pública. Quanto a esses objetivos, adianta-se que foi identificado choque entre o direito à privacidade e o interesse legítimo das empresas, conforme será visto no capítulo 1, bem como foram mapeados no capítulo 2 os limites de natureza, coleta, uso, tratamento, armazenamento e eliminação de dados pessoais definidos na LGPD e elencados os requisitos necessários para uso de dados pessoais oriundos de investigações internas nos acordos com a administração pública, no capítulo 3.

Partindo da hipótese de que há um possível choque entre o direito à privacidade dos trabalhadores e o interesse legítimo das empresas em conduzir investigações internas no âmbito de programas de *compliance*, pretende-se demonstrar que, a fim de que esses direitos sejam harmonizados, deve-se observar os requisitos e limites contidos na LGPD relativos à natureza, coleta e uso de dados pessoais para que sejam utilizados como prova da conduta na celebração de acordos com a administração pública.

Para alcançar o resultado esperado, o trabalho está dividido em cinco capítulos. O Capítulo 1 é destinado a introduzir o tema a ser tratado por meio da descrição do problema em questão, da apresentação da justificativa do estudo, seus objetivos gerais e específicos e sua estrutura. O Capítulo 2 é, de modo introdutório e conceitual, discorrerá sobre o direito à privacidade, a proteção de dados pessoais e os demais direitos fundamentais relacionados, bem como os fundamentos e princípios da LGPD. Em contrapartida, abordará, também, os possíveis

reflexos problemáticos na interface entre a lei e o interesse legítimo das empresas em celebrar acordos de cooperação com a administração pública. O Capítulo 3 é abordará os requisitos para uso das informações coletadas por meio das investigações internas na celebração de acordos com a administração pública e a LGPD, tratando especificamente de cada tipo de acordo ao abordar as condições para celebração destes. Além disso, será estudada a observância da LGPD quando da celebração de tais acordos, inclusive no que tange à ANPD e as possíveis sanções a serem aplicadas. Ainda, o Capítulo 4 é relacionará dados pessoais, *compliance* e investigações internas, tratando das etapas da proteção de dados pessoais, a responsabilidade civil prevista na LGPD e as sanções da ANPD. Por fim, o Capítulo 5 trará as conclusões alcançadas após os estudos das normas e doutrinas referentes ao tema deste trabalho.

2 O DIREITO À PRIVACIDADE, A LGPD E OS DIREITOS FUNDAMENTAIS FRENTE AOS INTERESSES LEGÍTIMOS DAS EMPRESAS PARA A CELEBRAÇÃO DE ACORDOS DE COOPERAÇÃO COM A ADMINISTRAÇÃO PÚBLICA

Diante do potencial choque entre o direito à privacidade - e os demais direitos fundamentais - e os interesses legítimos da empresa (ou o cumprimento de obrigação legal ou regulatória), faz-se necessário, para o presente trabalho, analisá-los separadamente e confrontá-los, para que sejam verificados eventuais contrapontos. Dessa forma, pretende-se iniciar a análise de modo a identificar um potencial choque entre o direito à privacidade e proteção de dados e o interesse legítimo das empresas.

Para isso, será analisada, em um primeiro momento, a LGPD como novo marco legal relativo ao direito à privacidade (2.1), conceituando e trazendo informações sobre o direito à privacidade (2.1.1), inclusive sua relação com os direitos fundamentais (2.1.2). Na segunda parte, serão abordados os possíveis reflexos problemáticos entre a LGPD e o interesse legítimo das empresas em celebrar acordos de cooperação com a administração pública (2.2), tratando dos requisitos gerais (2.2.1) e as novas diretrizes resultantes da LGPD para a celebração de tais acordos (2.2.2).

2.1 LGPD: O NOVO MARCO LEGAL RELATIVO AO DIREITO À PRIVACIDADE E AOS DIREITOS FUNDAMENTAIS NO BRASIL

Antes de tratar das características da LGPD, faz-se necessário realizar breve retrospecto histórico legislativo brasileiro em relação ao tema. Antes da entrada em vigor da Lei Geral de Proteção de Dados, havia apenas normas setoriais sobre o tema que criaram uma estrutura legal complexa, tais como: *(i)* a Constituição Federal; *(ii)* o Código de Defesa do Consumidor; *(iii)* a Lei de Acesso à Informação; *(iv)* o Marco Civil da Internet; *(v)* a Lei Carolina Dieckmann; *(vi)* a Lei do Cadastro Positivo; entre outras.

A Constituição Federal brasileira (artigo 5º, inciso X), apesar de não declarar expressamente a proteção dos dados, garante a inviolabilidade de direitos pessoais como a intimidade, a vida privada, a honra e a imagem[20]. Já a LGPD exige que as atividades que envolvem o processamento de dados pessoais obedeçam aos seguintes princípios: *(i)* finalidade;

[20] BRASIL. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: dezembro de 2020.

(ii) transparência; *(iii)* necessidade; *(iv)* segurança e prevenção; *(v)* responsabilidade; *(vi)* qualidade dos dados; *(vii)* suficiência; *(viii)* livre acesso; *(ix)* não discriminação; e *(x)* contribuição[21].

Percebe-se, portanto, a evolução da sociedade quanto à preocupação em lidar de forma responsável com questões como a prevenção e resposta à eventos de vazamento de dados pessoais. Apesar do Brasil disciplinar por muito tempo a proteção ao direito à privacidade em normas distintas, não garante a privacidade e a proteção de dados de forma abrangente, completa e estruturada. Sendo assim, surgiu a necessidade de criar uma norma geral e unitária: a LGPD.

Logo, para tratar da LGPD, inicialmente, será sucedida, no subitem a seguir (2.1.1), a análise conceitual e demais considerações sobre o direito à privacidade, relacionando-o aos demais direitos fundamentais em seguida (2.1.2).

2.1.1 Direito à privacidade: conceito e considerações iniciais

É importante conceituar privacidade devido às controvérsias que a cercam. Vale dizer que é um conceito amplo que apresenta muitas nuances, dispondo de pouco consenso entre os autores quanto aos termos utilizados. O principal entendimento é de que a intimidade é o núcleo da vida privada do indivíduo[22]. Mas intimidade e privacidade não são entendidas como sendo sinônimos? Na verdade, não.

Manoel Gonçalves Ferreira Filho[23] elucida a dificuldade de diferenciação entre vida privada e intimidade e, sendo a intimidade parte da vida privada, não são sinônimos. A vida privada envolve situações compartilhadas com grupos ou pessoas conforme a vontade do indivíduo, mas que ele não quer que sejam de conhecimento público[24]. Afinal, "consideram os juristas brasileiros que as expressões não são sinônimas, mas estão em uma relação de gênero e espécie, constituindo a intimidade um âmbito mais restrito da vida privada"[25].

---

[21] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: dezembro de 2020.
[22] VIDAL, Gabriel. Conceituação do direito à privacidade em face das novas tecnologias.
[23] FERREIRA FILHO, M. G. Curso de direito constitucional. 33.ed. rev. e atual. São Paulo: Saraiva, 2007. p. 296.
[24] MATEUCCI, C. R. F. Privacidade e internet. Revista de Direito Privado, São Paulo, ano 5, p.46-55, jul.-set. 2004.
[25] CARVALHO, A. P. G. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. Revista de Direito do Consumidor, São Paulo, N. 46, p.77-119, abr.-jun. 2003.

Assim, o vocábulo "privacidade" tenta conciliar os dois termos, segundo Manoel Gonçalves Ferreira Filho:

> De qualquer forma, em termos práticos, esta diferenciação apresenta reduzida importância uma vez que os efeitos jurídicos da violação da intimidade e da vida privada são idênticos, ensejando, no âmbito civil, o dever de reparação consistente no pagamento de indenização dos danos morais e patrimoniais sofridos pela vítima[26].

José Afonso da Silva[27] explica a preferência pelo termo "direito à privacidade", de forma genérica, para tratar de todas essas nuances, posicionamento firmado por outros doutrinadores também[28]. Dessa forma, é possível tratar a intimidade e a vida privada sem gerar incongruências.

Privacidade é, para Celso Bastos, a "faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano"[29]. Adicionalmente, para Gilberto Haddad Jabur, um atributo da privacidade é a faculdade de se excluir do conhecimento de terceiros as informações que o titular quer preservar para si próprio, seu direito de viver em isolamento sem ser submetido a uma publicidade indesejada[30].

Ademais, Marcelo Pereira analisa o conceito do direito à privacidade e conclui que "o direito à intimidade seria (...) o poder das pessoas de controlar suas informações pessoais, as quais, ainda que não formem parte da vida privada delas, possam revelar aspectos de sua personalidade"[31]. Sidney Guerra também diferencia intimidade e vida privada, conforme trecho abaixo:

> Assim, para melhor esclarecimento, verifica-se que a intimidade é algo a mais do que a vida privada, ou seja, a intimidade caracteriza-se por aquele espaço, considerado pela pessoa como impenetrável, intransponível, indevassável e que, portanto, diz respeito única e exclusivamente a pessoa, como, por exemplo, recordações pessoais, memórias, diários, etc. Este espaço seria de tamanha importância que a pessoa não desejaria compartilhar com ninguém. São os segredos, as particularidades, as

[26] FERREIRA FILHO, M. G. Curso de direito constitucional. 33.ed. rev. e atual. São Paulo: Saraiva, 2007. p. 296.
[27] SILVA, J. A. Curso de direito constitucional positivo. 29.ed. São Paulo: Malheiros, 2007. p. 206.
[28] VIANNA, C. S. M. Da privacidade como direito fundamental da pessoa humana. Revista de Direito Privado, São Paulo, ano 5, p.102-115, janeiro-março, 2004.
[29] BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. Comentários à Constituição do Brasil. São Paulo: Saraiva, 1989, vol. 2, p. 63.
[30] Ibidem.
[31] PEREIRA, Marcelo Cardoso. Direito à intimidade na internet. 2a ed. Curitiba: Juruá Editora, 2004, p. 140.

> expectativas, enfim, seria, o que vamos chamar de o 'canto sagrado' que cada pessoa possui. Já a vida privada consiste naquelas particularidades que dizem respeito, por exemplo, à família, problemas envolvendo parentes próximos, saúde física e mental etc. Seria então aquela esfera íntima de cada um, que vedasse a intromissão alheia. Entretanto, percebe-se que neste caso a pessoa poderia partilhá-la com as pessoas que bem lhe conviesse, sendo da família ou apenas um amigo próximo[32].

Com esse trecho, observa-se que a intimidade corresponde à uma esfera mais reservada do indivíduo, que deve sempre ser mantida em segredo, inacessível, de conhecimento apenas do titular. Enquanto a privacidade é todo ato humano externo na esfera da vida do indivíduo que quer que seja preservada de divulgação ou de conhecimento por terceiros em geral, que seja limitada a um círculo restrito de pessoas[33]. Sendo assim, da intimidade não participam outras pessoas, apenas o próprio indivíduo, e da vida privada participam as pessoas que possuem íntima convivência com o indivíduo, com acesso a informações pessoais.

No entanto, o direito à privacidade ganhou um viés mais dinâmico no contexto da sociedade em rede. Se antes era tido como um direito de ser deixado em paz (*right to be let alone*)[34], agora reflete o direito de o indivíduo conhecer, controlar, encaminhar e interromper o fluxo de informações a seu respeito[35]. O direito de ser deixado em paz é a afirmação mais representativa do direito à privacidade até hoje.

Justamente por isso, com a entrada em vigor da LGPD, as empresas devem se atentar muito mais, principalmente os *e-commerces* e as empresas de telemarketing, com o manuseio de dados pessoais. Deverá haver cuidados redobrados nas entrevistas de empregos e no recebimento de currículos, por exemplo, devendo evitar dados sensíveis relativos à etnia, religião, sexualidade etc. Além disso, os currículos não aproveitados pela empresa devem ser incinerados ou devolvidos aos candidatos, sendo vedada a distribuição para outras empresas sem a autorização do titular dos dados por escrito.

Ademais, a LGPD agregou grande valor ao aperfeiçoamento da ciência jurídica e do meio social no Brasil, tendo sido norteada pelo consentimento. Sendo assim, é um instrumento jurídico visando garantir maior segurança jurídica para empresas e usuários. Como forma de garantir isso, a LGPD possui escopo extraterritorial, fazendo com que entidades que não estão estabelecidas no Brasil, mas que coletam dados aqui, se sujeitem à nova lei (artigo 3º). Assim

---

[32] GUERRA, Sidney. O direito à privacidade na internet: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004, p. 55.
[33] ALONSO, Félix Ruiz. Op. cit., pp. 24-25.
[34] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harward LR, Harward, v. 4, n. 5, p. 193-220, 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: dezembro de 2020.
[35] RODOTÁ, Stéfano. A vida na sociedade de vigilância – a privacidade hoje. São Paulo: Renovar, 2008. p. 92.

como as organizações brasileiras com operações extraterritoriais devem observar as legislações internacionais sobre o tema, como é o caso do GDPR.

Diante do exposto, conclui-se que intimidade é a parte mais reservada do indivíduo restrita a apenas ele, enquanto a privacidade corresponde a atos humanos externos do indivíduo de conhecimento seleto, limitado ao desejo do indivíduo de divulgá-las. Dito isso, a proteção de dados, grosso modo, é a forma de garantir a possibilidade de os cidadãos determinarem individualmente a utilização e acesso de seus dados pessoais e evitar que cause quaisquer danos.

Após a análise conceitual e as considerações gerais expostas sobre o direito à privacidade, incluindo sua diferenciação de intimidade, faz-se necessário relacioná-los aos demais direitos fundamentais, conforme será feito no subitem seguinte, justamente pela previsão na Constituição Federal, em seu artigo 5º, inciso X, da inviolabilidade de direitos pessoais como a intimidade, a vida privada, a honra e a imagem, que estão relacionados a proteção dos dados.

2.1.2 A relação entre o direito à privacidade e os demais direitos fundamentais

Inspirada no modelo europeu, a LGPD preencheu a lacuna brasileira do tratamento de dados pessoais de pessoas naturais e jurídicas, seja de direito público ou privado. A lei cumpre com a finalidade de garantir a tutela dos direitos fundamentais de liberdade, privacidade e desenvolvimento da pessoa natural.

Diante da vulnerabilidade dos titulares dos dados e da falta de transparência em como esses dados são coletados e tratados, é importante destacar os fundamentos da proteção de dados definidos pelo legislador presentes no artigo 2º da LGPD:

> 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.[36]

[36] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: maio de 2020.

Com relação à proteção da privacidade, cabe à pessoa controlar sua vida privada, decidindo pela inclusão ou não de terceiros. Para esse fim, é preciso ter a autodeterminação informativa, que é a soma da manifestação de vontade do titular e do controle em prestar informações sobre os seus dados. Já a liberdade de expressão é assegurada até o limite em que não desencadeia violação de direito de terceiros.

Apesar de ser um dos fundamentos da LGPD, o direito à autodeterminação informativa não está previsto de forma expressa na Constituição Federal. Ele foi deduzido de outras garantias elencadas no documento, como o princípio da dignidade da pessoa humana (artigo 1º, III) e da inviolabilidade da intimidade e da vida privada (artigo 5º, X). Além disso, em seu artigo 5º, XII, há referência na CF à inviolabilidade de dados quanto à interceptação de correspondências e comunicações telefônicas. É importante destacar que, no âmbito das relações de trabalho, a autodeterminação informativa visa limitar o poder diretivo do empregador quanto à coleta, distribuição e armazenamento de dados do trabalhador[37].

Incorporado ao direito de privacidade, há os direitos da intimidade, da honra, da imagem - também associados à personalidade da pessoa humana[38], e os direitos de liberdade, como a livre iniciativa e o desenvolvimento econômico e tecnológico. Assim, fica evidente a correspondência da nova lei com o texto constitucional.

Segundo Sarlet, Marinoni e Mitidiero, considerando todos esses direitos que orientam a proteção da dignidade e da personalidade humana, o direito à privacidade é o mais importante: "...diversamente de outras ordens constitucionais, a Constituição Federal não reconheceu apenas um genérico direito à privacidade (ou vida privada), mas optou por referir tanto a proteção da privacidade, quanto da intimidade..."[39]. Ele é tido como um reflexo da personalidade humana, fundamentado pela proteção da dignidade. Portanto, a finalidade da LGPD é a proteção aos direitos fundamentais, percebida no artigo 2º, à frente de atividades que envolvam dados pessoais.

Soma-se a esse entendimento o de Mendes e Branco, que evidenciam o desmembramento do vínculo do direito à privacidade aos relacionamentos pessoais em geral,

[37] LAMBERTY, Andrey. ISAIA, Cristiano. SILVA, Rosane. Os desafios do processo e da jurisdição no Estado democrático de direito: elementos de uma teoria da decidibilidade adequada à proteção de dados pessoais do trabalhador. Revista Eletrônica de Direito Processual – REDP, Rio de Janeiro. Ano 14. Volume 21. Número 3. Setembro a Dezembro de 2020, p. 71.
[38] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 49-52.
[39] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. 7. ed. São Paulo: Saraiva, 2018, p. 467-468.

como o âmbito profissional[40]. Dessa forma, procura-se limitar condutas abusivas e ilícitas praticadas contra os indivíduos[41].

É importante destacar, aqui, a intimidade como circunscrita ao direito à privacidade. Ela compreende as relações mais íntimas dos indivíduos que podem ser ocultas até das pessoas mais próximas, vinculada ao direito a uma vida secreta e à reserva do ser humano sem intromissões[42].

Para Sarlet, Marinoni e Mitidiero (2018, p. 339), os direitos fundamentais são posições jurídicas que se mostram reconhecidas e, por consequência, devidamente protegidas na estrutura do direito constitucional interno dos respectivos Estados. Já Padilha (2018, p. 364) delimita que "Os direitos fundamentais são os direitos considerados indispensáveis à manutenção da dignidade da pessoa humana, necessários para assegurar a todos uma existência digna, livre e igual". São uma limitação popular ao Poder Público, em consonância com o Estado democrático de Direito.

Uma característica dos direitos fundamentais é a relatividade. Segundo Bahia (2017, p. 107), esses direitos não possuem caráter absoluto e podem ser relativizados em uma situação de conflito em face de outro direito. Outrossim, são direitos inalienáveis, ou seja, indisponíveis. Isso significa que o indivíduo não pode renunciar ou excluir seus direitos (Mendes e Branco, 2017, p. 135). Adicionalmente, Padilha (2018, p. 367) compreende serem os direitos fundamentais universais, devendo ser aplicados a todos, sem exceções. Ao passo que Bahia (2017, p. 107) defende que os direitos não atuam separadamente, possuindo caráter complementar.

Considerando esse caráter de relatividade dos direitos fundamentais, bem como a função da LGPD de proteger os direitos fundamentais nas atividades que envolvam dados pessoais, vale recordar uma questão levantada no capítulo 1: a relativização dos direitos fundamentais, prevalecendo o legítimo interesse das empresas para celebração de acordos de cooperação com a administração pública, não seria uma violação aos direitos de privacidade dos executivos, dos funcionários e até mesmo de terceiros, apesar de seu caráter de relatividade?

De início, a resposta seria que sim. No entanto, para responder a essa questão, é preciso contrabalancear todos os direitos "em jogo" e analisar as hipóteses em que poderão ser utilizadas a base legal do legítimo interesse, conforme será feito no adiante.

---

[40] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 12. ed. São Paulo: Saraiva, 2017, p. 245.
[41] BULOS, Uadi Lammêgo. Curso de Direito Constitucional. 8. ed. São Paulo: Saraiva, 2014, p. 571.
[42] BULOS, Uadi Lammêgo. Curso de Direito Constitucional. 8. ed. São Paulo: Saraiva, 2014, p. 571.

Diante do exposto ao longo do subitem 2.1, resumidamente, depreende-se que a intimidade é a parte mais reservada do indivíduo restrita a apenas ele, enquanto a privacidade corresponde a atos humanos externos do indivíduo de conhecimento seleto, limitado ao desejo do indivíduo de divulgá-las. Dito isso, a proteção de dados, grosso modo, é a forma de garantir a possibilidade de os cidadãos determinarem individualmente a utilização de seus dados pessoais e evitar que cause quaisquer danos.

No caso concreto, portanto, percebe-se que os direitos fundamentais, indispensáveis à manutenção da dignidade da pessoa humana, podem colidir com os direitos fundamentais de outros particulares, como no caso do direito à privacidade dos empregados e o poder diretivo do empregador devido à necessidade de informações relevantes para realização e continuidade de contratações.

Além do mais, são os direitos da intimidade, da honra, da imagem, de liberdade, da livre iniciativa e do desenvolvimento econômico e tecnológico que orientam a proteção da dignidade e da personalidade humana, sendo o direito à privacidade o mais importante, já que é tido como um reflexo da personalidade humana, fundamentado pela proteção da dignidade. Por isso, a finalidade da LGPD é a proteção aos direitos fundamentais, percebida no artigo 2º, à frente de atividades que envolvam dados pessoais.

De forma a dar sequência à pesquisa, será abordado no próximo subitem justamente os possíveis reflexos decorrentes da interposição das questões relativas ao direito à privacidade e aos direitos fundamentais, expostas acima, quando do uso do legítimo interesse para a celebração de acordos de cooperação com a administração pública. Isso se faz necessário, principalmente, por esse caráter da LGPD de proteger os direitos fundamentais no que se refere a atividades que envolvam dados pessoais.

2.2 OS POSSÍVEIS REFLEXOS PROBLEMÁTICOS NA INTERFACE ENTRE A LGPD E O INTERESSE LEGÍTIMO DAS EMPRESAS PARA A CELEBRAÇÃO DE ACORDOS DE COOPERAÇÃO COM A ADMINISTRAÇÃO PÚBLICA

Diante do exposto até o momento sobre o direito à privacidade e a LGPD, deve-se citar outro ponto igualmente relevante que pode confrontar com os direitos fundamentais das pessoas: o interesse legítimo das empresas. Soma-se a isso a possibilidade de serem realizadas investigações internas conduzidas por entidades privadas com a finalidade de cumprir com

alguma obrigação legal. Vale dizer que a base legal do legítimo interesse será exposta de modo geral, sendo tratada de forma mais profunda no capítulo 4.

Isso é percebido frequentemente no âmbito das relações de trabalho. As Tecnologias da Informação e da Comunicação (TIC) permitiram o acesso, o uso e a distribuição de dados pessoais de funcionários e, consequentemente, a vigilância por meios eletrônicos. Ocorre em todas as etapas do contrato de trabalho, iniciando-se na fase pré-contratual, com o armazenamento de dados sensíveis coletados na entrevista e em pesquisas investigativas. Durante a vigência do contrato, a empresa possui acesso a e-mails privados, monitora aplicativos de mensagens instantâneas e câmeras nos locais de trabalho, rastreia notebooks e smartphones, utiliza-se de softwares "espiões" e muito mais. Em suma, afrontam o direito à privacidade do empregado continuamente. Por fim, na fase pós-contratual, utilizam os dados dos ex-funcionários para integrar bancos de dados para as mais diversas finalidades.

Fato é que o legítimo interesse tem sido caracterizado pelo sistema de proteção de dados europeu e pela GDPR como uma flexibilização das bases legais de tratamentos de dados. Segundo Bioni[43], a base legal do legítimo interesse torna-se ainda mais relevante no contexto do surgimento de novas tecnologias e da economia baseada no uso intensivo de dados.

Inicialmente, na Europa não foram detalhados os critérios de aplicação da base legal do legítimo interesse em relação à proteção de dados. No entanto, a GDPR utiliza uma técnica normativa prescritiva com eficácia em todo o bloco europeu que estabeleceu a necessidade de estabilização do conceito jurídico de legítimo interesse. A necessidade de previsão legal de sua aplicação se deu por este ser um denominador comum entre os titulares de dados, os agentes reguladores e a cadeia de tratamento de dados.

A respeito da lei brasileira, vale destacar que bases legais são hipóteses da lei que autorizam a empresa a realizar operações com os dados pessoais que possui. O consentimento e os contratos são outras duas principais bases legais da LGPD. No entanto, o legítimo interesse é uma das bases legais mais relevantes. Isso ocorre devido ao seu caráter de elevada flexibilidade.

Entretanto, devem ser observados os requisitos elencados no artigo 10 da LGPD para que seja aplicado o teste de proporcionalidade do legítimo interesse, quais sejam: *(i)* a verificação da legitimidade do interesse por parte do controlador dos dados; *(ii)* a necessidade do uso dos dados coletados; *(iii)* o balanceamento entre a obtenção de dados pelo controlador e

[43] BIONI, Bruno Ricardo, Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p.248-267.

a disponibilização do dado pelo titular; e *(iv)* a transparência do procedimento e da finalidade dos dados coletados com o titular e os mecanismos de diminuição de riscos. Esses requisitos devem ser preenchidos para que este instituto seja utilizado.

Não é fácil cumprir com todos esses requisitos para que seja deixado de lado o consentimento do titular dos dados. Um dos principais fundamentos para utilização da base legal do legítimo interesse é quando o consentimento do usuário é muito difícil de ser obtido ou pode ser considerado desnecessário. Ademais, outro forte argumento é a existência de um impacto mínimo no indivíduo ou uma justificativa convincente para a utilização dos dados pessoais.

Diante do panorama exposto, apesar de o consentimento e os contratos serem as duas principais bases legais da LGPD, o legítimo interesse é uma das mais relevantes, devido ao seu caráter de elevada flexibilidade. Esta base legal, por sua vez, se mostrou como uma medida capaz de flexibilizar as relações de dados na Europa e, no Brasil, foi utilizada a mesma técnica na LGPD.

Não obstante, há que se analisar esse choque entre os direitos fundamentais de privacidade e proteção de dados pessoais e o interesse legítimo das empresas, principalmente quanto à realização de investigações internas e a celebração de acordos de cooperação com a administração pública. Para isso, inicialmente, serão analisados os requisitos para celebração destes acordos (2.2.1) e em seguida, serão tratadas as novas diretrizes da LGPD aplicáveis às investigações internas (2.2.2).

2.2.1 *Acordos de cooperação com a administração pública: justificativas, pilares e requisitos gerais*

Para fins desse trabalho, considera-se Acordo de Leniência aquele celebrado entre uma autoridade pública investigadora e um agente privado, seja pessoa física ou jurídica, com o qual será concedida extinção ou abrandamento da penalidade aplicável ao agente pela autoridade. A condição é que, em troca, a autoridade receba provas e colaboração material e processual durante as investigações[44]. Por sua vez, o Programa de Leniência é a estrutura que providencia incentivos da autoridade pública investigadora para atrair os agentes privados a procurarem negociação de Acordos de Leniência[45].

[44] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 30.
[45] Ibidem, p. 31.

É importante dizer que, neste momento, serão abordados os aspectos gerais dos acordos de cooperação que podem ser celebrados com a administração pública, bem como seus requisitos. As especificidades e os tipos de acordo serão abordados com maiores detalhes no capítulo 4. Inicialmente, a fim de fundamentar a instituição dos Programas de Leniência, serão tratadas suas justificativas.

Dentre as justificativas para instituição de um Programa de Leniência, segundo Athayde[46], pode-se citar: *(i)* detecção de práticas ilícitas; *(ii)* a obtenção de provas; *(iii)* a eficiência e a efetividade investigativa; *(iv)* a cessação da infração; *(v)* a sanção dos demais infratores; *(vi)* a reparação e o ressarcimento dos danos; e *(vii)* a dissuasão de práticas ilícitas futuras.

Considerando que, geralmente, atos ilícitos como cartel, corrupção, lavagem de dinheiro, crimes no mercado financeiro, organizações criminosas, entre outros, são de difícil detecção pelas autoridades investigadoras, o infrator é favorecido por ser justamente quem mais sabe sobre o ilícito cometido. Dessa forma, uma importante maneira de se obter tais informações é diretamente com os envolvidos, por investigação direta ou celebração de acordos de cooperação[47].

Quanto à obtenção de provas, estas poderiam ser obtidas por outros meios, como medidas cautelares de busca e apreensão, sem colaboração do infrator. No entanto, às vezes é necessário auxílio para compreendê-las, por, por exemplo, serem cifradas. Além disso, essa medida pode ajudar a identificar mais facilmente os demais infratores.

Outro benefício dos Programas de Leniência é o ganho de eficiência e a efetividade investigativa por permitirem a realização de uma investigação mais substancial em menor tempo e empregando menos recursos humanos e financeiros. Assim, a probabilidade de se obter melhores resultados na investigação é muito maior. Isso ocorre justamente pela justificativa da obtenção de provas, que permite acesso a informações e documentos relacionados a práticas de difícil detecção e, consequentemente, reduz custos de iniciação dos casos, instrução processual e litigância em eventuais questionamentos judiciais da condenação[48]. Para Lorenz, uma das principais vantagens é proporcionar resultado semelhantes ou melhores custando relativamente pouco[49].

---

[46] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 26.
[47] LORENZ, Moritz. *An introduction to EU competition law*. Cambridge University Press, 2013. P. 352-353.
[48] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 44.
[49] LORENZ, Moritz. *An introduction to EU competition law*. Cambridge University Press, 2013. P. 352-353.

Percebe-se, também, um benefício quase que imediato para a sociedade quando celebrados acordos, visto que geralmente envolvem cláusulas que obrigam os agentes a cessarem as práticas ilícitas antes da celebração do acordo, acabando por reduzir os prejuízos aos cidadãos.

Complementarmente, prevalecem os interesses dos cidadãos em ver os ilícitos desvendados, cessados e punidos sobre o interesse de sancionar todos os agentes infratores envolvidos no ilícito. Por isso, é permitido que alguns agentes colaborem e celebrem acordos e outros não[50].

Quanto à reparação e ao ressarcimento dos danos, o Programa de Leniência pode subsidiar, de forma direta ou indireta, essas ações em face dos infratores. Dessa forma, os Acordos de Leniência garantem um retorno positivo para a sociedade também. Além disso, essa pode ser uma circunstância atenuante para a penalização de empresas investigadas por cartel, desde que devidamente comprovada, conforme dispõe o artigo 13 da Resolução n° 21/20218 do Cade[51].

Por fim, a última justificativa é a dissuasão de práticas ilícitas futuras. Isso ocorre já que o Programa de Leniência acaba por aumentar os riscos de práticas ilícitas serem descobertas por facilitar a detecção dessas práticas e realizar investigações mais rápidas e robustas - consequência de possuir informações e documentos de forma colaborativa.

Ademais, é importante tratar, também, dos pilares para estruturação desses programas, que objetivam a sua efetividade. Os 3 pilares para estruturação dos Programas de Leniência, também segundo Athayde[52], são: *(i)* alto risco de detecção da prática; *(ii)* receio de severas punições; e *(iii)* transparência, previsibilidade e segurança jurídica.

Primeiramente, o alto risco de detecção da prática ilícita é explicitado diante do compromisso das agências de investigar as práticas que serão objeto de acordos. Para isso, devem ser empregados métodos reativos e proativos complementarmente[53]. Os métodos reativos elencados por Athayde[54], seriam: *(i)* recebimento de denúncias, seja da população em geral ou de informantes; *(ii)* colaborações premiadas; e *(iii)* os próprios acordos de leniência.

---

[50] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 48.
[51] Idem; MAIOLINO, Isabela. Ressarcimento voluntário de danos e acordos no Cade – O que isso significa para as ações de reparação de dano por conduta anticompetitiva no Brasil? Portal, Jota, 10 dez. 2018.
[52] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 26.
[53] Ibidem. p. 67.
[54] Ibidem. p. 65.

Enquanto alguns dos proativos seriam[55]: *(i)* análises econômicas de mercado; *(ii)* programas de educação e sensibilização sobre a ilegalidade de determinadas condutas; *(iii)* cooperação com outras autoridades nacionais e internacionais de repressão a práticas ilícitas; *(iv)* monitoramento da atividade de alguns players; e *(v)* implementação e filtros econômicos.

Quanto ao receio de severas punições, esse é um fator essencial pois as sanções devem ser significativas para que seja um incentivo à colaboração e seja visto como benefício. A pena é um fator persuasivo, considerando que:

> No Brasil, cartel é crime, nos termos do art. 4º da Lei 8.137/90, punível com pena de reclusão de dois a cinco anos e multa. A lavagem de dinheiro, por sua vez, é crime punível com reclusão de três a dez anos e multa. Ainda, participar em organização criminosa é punível com reclusão de três a oito anos e multa. Ademais, a corrupção ativa ou passiva é punível com pena de dois a doze anos e multa[56].

Dessa forma, devem ser alinhados o poder punitivo das autoridades, como as Polícias Federal e Civil e os Ministérios Públicos, a fim de que fique claro aos infratores e seja afastada a ideia de que possíveis penalidades podem ser compensadas pelas potenciais recompensas da infração.

Por fim, o terceiro pilar se trata da transparência, previsibilidade e segurança jurídica que pairam as negociações e assinaturas de acordos. Vale destacar o papel dos guias divulgados pelas autoridades que tencionam sanar dúvidas sobre os programas de leniência. No contexto da proteção de dados, algumas das principais questões que devem ser esclarecidas são: *(i)* o risco de vazamento das informações; *(ii)* como se dará o manuseio e a entrega das informações e dos documentos; *(iii)* quem vai ter acesso e como terá acesso ao banco de dados que contém as informações fornecidas pelo leniente; *(iv)* como será garantido o sigilo das informações; e *(v)* se existe a possibilidade de interromper a colaboração e não ser prejudicado pelas informações prestadas. Sendo assim, para que os colaboradores tenham segurança jurídica quanto ao processo de negociação, a autoridade deve ser transparente e previsível.

Vale destacar, também, o papel dos acordos de cooperação com a administração pública no âmbito das investigações internas realizadas por programas de *compliance*. Diante da constatação de eventuais práticas ilícitas que tenham sido praticadas, seja por meio de auditoria interna ou denúncia, as empresas buscam cada vez mais negociar acordos de cooperação com

[55] Ibidem. p. 66.
[56] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 70.

os órgãos reguladores[57]. Dessa forma, evitam multas e penalidades futuras, preservam a imagem da empresa e têm oportunidade de implantar eventuais melhorias que forem apontadas. O Poder Público também se beneficia da celebração desses acordos, visto que a cooperação das empresas infratoras ajuda a alcançar resultados mais práticos e céleres, sendo menos custoso para a administração pública visto que menor o esforço investigativo.

Para isso, é necessária a capacitação dos envolvidos, principalmente das áreas que acompanharão o desdobramento dos trabalhos de investigação e do acordo. Uma boa estrutura de *compliance* também facilitará os trabalhos da organização, conforme veremos nesta pesquisa, já que será necessário conciliar grupos interdisciplinares, além de prevenir e mitigar riscos.

Dentre a condições para celebração de acordos de leniência, conforme os artigos 16, II, da Lei nº 12.846/2013 (Lei Anticorrupção) e 28, II, do Decreto nº 8.420/2015, também está a identificação dos envolvidos em atos infracionais contra a administração pública e a obtenção de documentos comprobatórios de tais práticas ilícitas. Para isso, a empresa, na posição de colaboradora, deve iniciar a fase de investigação interna para coleta de informações e provas logo após a celebração do acordo.

Ademais, nos acordos de cooperação premiada os colaboradores têm o dever geral de colaborar efetiva e voluntariamente de forma a prevenir novos crimes, recuperar o produto do crime e localizar a vítima, bem como revelar a estrutura da organização criminosa e identificar os coautores.

Diante do exposto, conclui-se que são 5 os requisitos para a celebração de acordos, quais sejam: *(i)* a manifestação de interesse em cooperar para a apuração de ato lesivo específico, quando tal circunstância for relevante; *(ii)* a cessação da prática da irregularidade investigada; *(iii)* a cooperação com as investigações, identificando os demais envolvidos na infração quando couber; *(iv)* o fornecimento de informações e documentos que comprovem a infração; e *(v)* o comprometimento de implementar ou melhorar mecanismos internos de integridade (*compliance*), auditoria, incentivo às denúncias de irregularidades e à aplicação efetiva de código de ética e de conduta na organização.

Apesar de cada um dos acordos de cooperação possuírem regimes jurídicos distintos, com atores, procedimentos e benefícios específicos, eles possuem uma coisa em comum: a possibilidade de transação através da lógica pragmática de estímulo à cooperação em troca de

[57] Deloitte. Orientações para celebração de acordos de cooperação por empresas. IBDEE, agosto de 2018. Pesquisa "Acordos de Cooperação – Percepção do Empresariado sobre o Tema e Práticas Adotadas", p. 6.

algum benefício[58]. A variedade de acordos de cooperação possíveis e suas particularidades serão tratadas no próximo capítulo deste trabalho.

Após a exposição dos requisitos para celebração dos acordos, inclusive das suas justificativas e pilares, é necessário compreender as diretrizes da LGPD que devem ser aplicadas às investigações internas e às etapas da celebração de acordos diante da alta maleabilidade de dados pessoais, conforme será exposto no subitem a seguir.

2.2.2 *As novas diretrizes da LGPD aplicáveis às investigações internas para celebração de acordos com a administração pública*

A nova lei trata em seu artigo 5º, X do rol exemplificativo das atividades consideradas como tratamento de dados pessoais, que será discutido com maior profundidade no próximo capítulo. Ficam submissas ao cumprimento da LGPD as pessoas físicas que tratem de dados pessoais com finalidade econômica e as pessoas jurídicas. No entanto, há exceções ao enquadramento da lei, como o tratamento de dados realizados por pessoas físicas para fins estritamente particulares e não econômicos, bem como para fins acadêmicos, jornalísticos, artísticos, de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais, consoante os artigos 3º e 4º.

A LGPD elenca 4 figuras principais relativas aos dados pessoais em seu artigo 5º, V ao VIII: *(i)* o titular - pessoa física ao qual o dado se refere; *(ii)* o controlador - pessoa a quem compete as decisões referentes ao tratamento, seja natural ou jurídica, de direito público ou privado; *(iii)* o operador - pessoa que realiza o efetivo tratamento em nome do controlador, seja natural ou jurídica, de direito público ou privado; e *(iv)* o encarregado - pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre as outras 3 figuras citadas e a Autoridade Nacional de Proteção de Dados (ANPD). Por sua vez, esse é o órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no território nacional (artigo 5º XIX e 55-A) e está diretamente vinculado à administração pública federal.

O tratamento de dados pessoais deve observar os princípios expostos no artigo 6º da LGPD já citados. Além disso, o artigo 7º expõe as possibilidades legais de enquadramento dessa situação, conforme abaixo:

> I - mediante o fornecimento de consentimento pelo titular;

[58] Deloitte. Orientações para celebração de acordos de cooperação por empresas. IBDEE, agosto de 2018. Pesquisa "Acordos de Cooperação – Percepção do Empresariado sobre o Tema e Práticas Adotadas", p. 7.

> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O não cumprimento de uma das dez bases legais evidenciadas acima pode resultar em sanções administrativas (artigo 52 da LGPD) a serem aplicadas pela ANPD aos agentes envolvidos, gradativa, isolada ou cumulativamente, quais sejam: *(i)* multas de até R$ 50 milhões; *(ii)* publicização da infração; *(iii)* bloqueio e eliminação de dados pessoais; e *(iv)* suspensão de banco de dados e proibição do exercício de atividades de tratamento de dados.

No que diz respeito às empresas, o acesso às informações e o tratamento dos dados pessoais inerentes às investigações internas para fins de cumprimento de acordos está respaldado no inciso II do artigo descrito acima, desde que fundamentado. Ao receber tais informações, o Poder Público deve agir conforme o artigo 7º, inciso III. Para evidenciar o cumprimento dos princípios já citados previstos na lei, as empresas devem elaborar relatórios das operações de tratamento de dados pessoais, indicando quais dados são tratados, a finalidade, a forma de coleta, o plano de segurança da informação e o operador, de acordo com os artigos 37 a 38 da lei.

Isso acontece para que seja verificada a real necessidade de uso dos dados e garantida a segurança quanto ao uso adequado e lícito, de forma a evitar prejuízos e violações ao titular dos dados, bem como realizar a prestação de contas (*accountability*) pelo controlador - que devem ser somadas à atualização das políticas de privacidade e proteção de dados.

Ainda, não pode ser deixada de lado a necessidade da empresa colaboradora, como controlador de dados pessoais, nomear um encarregado para coordenar o tratamento de dados e realizar as comunicações com os titulares e a ANPD.

Ademais, é possível enquadrar eventuais investigações iniciadas antes da celebração de acordo na base legal do legítimo interesse (artigo 7º, IX da LGPD), já que a empresa possui um interesse legítimo de investigar eventuais desvios de condutas que possam evidenciar práticas ilícitas e gerar prejuízos. A condição é que sejam respeitadas a legítima expectativa do titular dos dados, os direitos fundamentais e os demais princípios da lei.

O artigo 7º da LGPD expõe as situações em que pode ser realizado o tratamento de dados pessoais – que devem obedecer aos princípios elencados no artigo 6º da referida lei. Apesar de prever inúmeras situações em que é permitido, como com o consentimento do titular, para o controlador cumprir obrigação legal ou regulatória e para atender aos interesses legítimos do controlador ou de terceiros, a lei é bastante clara quanto à sua condição: exceto no caso de prevalecerem os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Diante do exposto, depreende-se que a proteção de dados é a forma de garantir a possibilidade de os cidadãos determinarem individualmente a utilização de seus dados pessoais e evitar que cause quaisquer danos. No entanto, os direitos fundamentais e de privacidade podem colidir com os direitos fundamentais de outros particulares, como no caso do direito à privacidade dos empregados e o poder diretivo do empregador.

Nesse sentido, busca-se, neste trabalho, uma resposta íntegra e coerente – que pretende-se seja apresentada no capítulo 5 - relativa à harmonização do conflito percebido entre o direito à privacidade e o interesse legítimo das empresas na coleta e processamento de dados dos colaboradores a fim de conduzir suas atividades econômicas de forma mais eficiente, diante do potencial lesivo de acesso, armazenamento e distribuição de seus dados pessoais, principalmente quanto ao seu uso para a celebração de acordos com a administração pública.

De forma a dar sequência ao estudo, serão abordados, no próximo capítulo, os requisitos para uso das informações coletadas nas investigações internas, tratando especificamente de cada tipo de acordo possível de ser celebrado. Na segunda parte, serão abordadas questões relativas à observância da LGPD quando da celebração destes acordos, bem como o papel da ANPD.

3 LGPD: ETAPAS PARA PROTEÇÃO DE DADOS PESSOAIS, A RESPONSABILIDADE CIVIL PREVISTA E AS SANÇÕES APLICÁVEIS AO SEU DESCUMPRIMENTO

Após fundamentar a importância de garantir o direito à privacidade e sua relação com os demais direitos fundamentais, principalmente frente ao conflito existente entre o titular dos dados e o uso destes pela empresa pela via do legítimo interesse, foram especificados os tipos de acordo e as condições gerais para sua celebração, inclusive para que sejam observadas as diretrizes previstas na LGPD. No entanto, ainda é preciso mapear os limites de natureza, coleta, uso, tratamento, armazenamento e eliminação de dados pessoais definidos na LGPD.

Para isso, serão abordadas as etapas de proteção de dados pessoais (3.1), incluindo como é a natureza (3.1.1), como deve ser o processo de coleta (3.1.2), uso, tratamento (3.1.3), armazenamento (3.1.4) e eliminação (3.1.5) dos dados pelas empresas. No subitem a seguir, é tratada a responsabilidade civil decorrente do não cumprimento das diretrizes da LGPD (3.2), discorrendo sobre o posicionamento jurisprudencial quanto à responsabilidade civil pela má gestão de dados (3.2.1) e as sanções aplicáveis pela ANPD nesses casos (3.2.2). É importante dizer que não se pretende tratar a fundo e exaurir todas as questões relativas à essas etapas, apenas expor, de forma sucinta, informações necessárias para situar o leitor e demonstrar a conjuntura total.

3.1 AS ETAPAS DA PROTEÇÃO DE DADOS PESSOAIS NOS TERMOS DA LGPD

Com o aumento do fluxo de informações presente na sociedade, aumentou-se, também, a necessidade de compreensão dos efeitos jurídicos oriundos desse novo contexto, principalmente quanto aos deveres de transparência e de informação com o titular dos dados. Fato é que diversas normas dispersas dispõem de alguma forma de algumas das etapas de proteção de dados pessoais. Sendo assim, estas normas serão expostas brevemente, a fim de garantir uma compreensão geral, antes de serem expostas as etapas, de fato, da previstas pela LGPD.

São os pilares do direito à informação presentes no artigo 5º, inciso XIV da Constituição Federal de 1988: *(i)* o direito de informar; *(ii)* o direito de se informar; e *(iii)* o direito de ser informado. Ademais, o inciso XXXIII fala especificamente das situações em que a informação pretendida deve constar de banco de dados, cadastros públicos ou de caráter público.

Relativa à legislação consumerista, o Código de Defesa do Consumidor (Lei no 9.078, de 11 de setembro de 1990) trata da privacidade e da segurança dos consumidores, tendo estabelecido uma Política Nacional das Relações de Consumo, com foco na transparência e na proteção dos interesses dos consumidores. Em seu artigo 43, assegura ao consumidor o acesso às informações sobre ele armazenadas em cadastros e bases de dados. Foram os princípios do CSC que sedimentaram a criação da LGPD.

O próprio Marco Civil da Internet já havia assegurado aos usuários da internet o direito a informações claras sobre as etapas de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais. Apesar da previsão em outras normas, conforme exposto, que visam proteger informações dos indivíduos, foi a LGPD que unificou e tratou com pertinência da proteção de dados pessoais. Sendo assim, serão analisadas nos próximos subitens, com maior profundidade, as etapas de proteção de dados pessoais que envolvem: a natureza (3.1.1.), a coleta (3.1.2.), o tratamento (3.1.3.), o armazenamento (3.1.4.) e a eliminação de dados pessoais previstos na LGPD (3.1.5.).

3.1.1 A natureza dos dados pessoais

Inicialmente, quanto à natureza dos dados e conforme o artigo 5º da LGPD, eles podem ser: *(i)* dados pessoais; *(ii)* dados pessoais sensíveis; e *(iii)* dados anonimizados. Dados pessoais são informações pertencentes a alguém que podem ser relacionadas a identificação ou possibilitar a identificação de alguém, de modo individualizado. Alguns exemplos são: o nome completo, RG, CPF, passaporte, CNH, endereço, telefones, e-mail, endereço de IP, data de nascimento e localização via GPS. Pouco importa se a natureza dos dados é física ou virtual, a LGPD as protege da mesma forma.

Já os dados sensíveis são dados pessoais que podem dar margem para alguma discriminação ou preconceito, podendo comprometer a privacidade do indivíduo. São exemplos: a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde, vida sexual genético ou biométrico, quando vinculados a uma pessoa natural. Por isso, suas regras são ainda mais rigorosas, já que pretende a tutela das características essenciais da pessoa humana[59].

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

Devido a sua posição de vulnerabilidade, os dados pessoais de crianças e adolescentes possuem regras específicas de tratamento. Vale dizer que, conforme o artigo 2º do Estatuto da Criança e do Adolescente, criança é a pessoa com até doze anos de idade incompletos e adolescente aquela que possui entre doze e dezoito anos[60]. Feita essa diferenciação, é necessário tratar de como deve ser a coleta de tais dados, conforme será feito a seguir.

3.1.2 A coleta dos dados pessoais

Quanto à coleta de dados pessoais, é importante destacar que devem ser coletados apenas os dados que forem essenciais para a segurança e/ou gestão da empresa. Sendo assim, não devem ser coletados dados que não possuem uma finalidade concreta para a empresa, e esse requisito deve ser observado principalmente quanto aos dados sensíveis. Ademais, a LGPD determina, em seu artigo 21, que a coleta de dados pessoais referentes ao exercício regular de direitos não pode ser utilizada em prejuízo do titular.

Notadamente, a LGPD, em seu artigo 18, prevê 9 modalidades de direitos do titular de dados, quais sejam:

> 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, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> 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.

No que diz respeito ao inciso IV acima, anonimização é o processo de desvinculação do dado a uma pessoa específica e identificável. Outro ponto relevante é a possibilidade de o titular

[60] BRASIL. Lei no 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente (ECA). Brasília, DF: Presidente da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: junho de 2020.

solicitar a portabilidade de dados. A possibilidade de revogar o consentimento, que deve ser manifestada de forma expressa, ganha grande destaque também, garantindo o direito do titular de restringir o tratamento de seus dados.

Os titulares podem pleitear tais direitos de forma administrativa, junto à agência reguladora de dados pessoais, a ANPD (artigo 18, §1º), e perante os organismos de defesa de consumidor (artigo 18, §8º). Também poderá requerer a defesa destes direitos em juízo, de forma individual ou coletiva (artigo 22). Autorizada a coleta dos dados pessoais, as atenções devem ser focadas no tratamento deles, que pode apresentar grandes dificuldades às empresas, consoante será tratado no subitem seguinte.

3.1.3 O tratamento dos dados pessoais

A priori, a LGPD prevê o consentimento do titular dos dados pessoais para que haja seu tratamento. Para isso, não basta que seja dada autorização quando da coleta dos dados, mas, sim, que seja garantido ao titular conhecimento de como seus dados serão tratados e para qual finalidade. Nas empresas, é comum o uso de ferramentas que coletam informações que são consideradas pessoais. Isso ocorre para garantir a segurança destas e de seus próprios dados. No entanto, é indispensável o consentimento de todos os titulares dos dados que a empresa coleta.

A Seção III da LGPD se dedica ao tratamento de dados de crianças e adolescentes, que precisam de consentimento não apenas do indivíduo, mas de seus pais/responsáveis legais. Há apenas uma exceção para que os dados sejam coletados sem consentimento: quando serão utilizados para contatar os pais/responsáveis legais de uma criança, desde que não sejam armazenados após o uso. Soma-se a isso o fato de que se deve publicitar o método de tratamento de dados de crianças coletados por empresas, como são tratados e por quê.

Na redação do artigo 7º da LGPD, tem-se a autorização de tratamento em função de consentimento, devendo ser livre, informada e inequívoca. Isto é, os titulares devem ter direito a uma escolha efetiva sobre que dados desejam autorizar o tratamento, devendo ser informados dos riscos a que podem estar sujeitos e das medidas que serão tomadas pelos agentes de tratamento para mitigar esses riscos. É preciso ter cautela com o tratamento de dados baseado no silêncio ou na negativa do titular, pois assim não há consentimento expresso e é ilegítimo.

Outra base para o tratamento de dados é o cumprimento de obrigação legal ou regulatória por parte do controlador, em que não mais será necessário o consentimento do titular. Compreende-se por obrigação legal aquelas previstas em leis federais, estaduais ou

municipais, decretos, resoluções, determinações internacionais, entre outros, excetuadas as obrigações contratuais.

A LGPD privilegia as instituições públicas em seus incisos II e III do artigo 7º, ao sobrepor o cumprimento de obrigações junto ao Poder Público ao direito dos titulares de disporem livremente sobre seus dados, não havendo necessidade de consentimento por parte do titular. Sendo assim, é autorizado o tratamento de dados pessoais pela administração pública, bem como o uso compartilhado de dados necessários à execução de políticas públicas.

A justificativa se dá pelas pretendidas melhorias a serem destinadas à sociedade ao cumprir com a finalidade de executar políticas públicas, mesmo burlando o mais importante requisito da proteção de dados pessoais. Ao menos o Poder Público deve observar o capítulo IV da LGPD ao compartilhar dados necessários.

Já o artigo 7º da lei em questão prevê a possibilidade de tratamento de dados pessoais quando necessário para execução de contrato ou de procedimentos pré-contratuais, desde que a pedido do titular dos dados. É o caso do titular que retoma parte de sua autodeterminação informativa ao autorizar o tratamento de seus dados para contrair contrato de seu interesse. O mesmo acontece no inciso VI, que trata do exercício regular de direitos em processo judicial, administrativo ou arbitral. Esta possibilidade de tratamento se baseia nas previsões constitucionais do artigo 5º de inafastabilidade da apreciação pelo Poder Judiciário (inciso XXXV) e da ampla defesa e contraditório (inciso LV).

Ainda, é autorizado o tratamento de dados pessoais sem consentimento, desde que tenha a finalidade de proteger a vida ou a incolumidade física do titular ou de terceiros. Maldonado[61] expõe muito bem com o seguinte exemplo:

> "A obtenção de dados de geolocalização de dispositivos de telefone celular, com o objetivo de tentar localizar eventuais vidas que possam estar no meio dos escombros, após determinado incidente. Igualmente, situações em que pessoas possam ter sido sequestradas ou estejam perdidas das suas famílias podem ensejar tentativas de obtenção de dados de geolocalização, a fim de identificar os titulares."

Soma-se à essas possibilidades a de tratamento de dados sem consentimento do titular para: *(i)* proteção do crédito, desde que observado o disposto na Lei do Cadastro Positivo e o Código de Proteção e Defesa do Consumidor; e *(ii)* tutela da saúde em procedimento realizado por profissionais da área de saúde ou por entidades sanitárias.

[61] MALDONADO, Viviane Nóbrega. BLUM, Renato Opice, coordenadores. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 185.

Por fim, dados pessoais podem ser tratados, também, para atender aos interesses legítimos do controlador ou de terceiros, excetuando-se os casos em que prevalecem direitos e liberdades fundamentais do titular que exijam a proteção desses dados. As questões que envolvem esta base legal são soturnas. Não há definição de um limite claro por parte da legislação quando se envolve o tratamento de dados por legítimo interesse de terceiro, que trata no artigo 10º apenas da figura do controlador.

Enfatiza-se que, apesar de não ser requisitado consentimento do titular nos casos acima, restam guardados os demais direitos, como o de informação. Sendo assim, não são dispensados os deveres dos agentes de tratamento elencados na lei. O artigo 5º da LGPD define os agentes do tratamento de dados pessoais como: o controlador e o operador, conforme tratado anteriormente.

Consoante exposto, conclui-se que o controlador é o principal tomador de decisões relacionadas aos dados pessoais coletados. Outras funções realizadas por ele são: *(i)* determinar a finalidade da coleta dos dados; *(ii)* controlar a forma como os dados serão coletados e usados; *(iii)* selecionar quais dados serão coletados e de quem; *(iv)* definir quanto tempo os dados ficarão armazenados; e *(v)* estabelecer quem terá acesso aos dados. Essa é a pessoa responsável por proteger os dados dos titulares e, consequentemente, possui muitas das responsabilidades previstas na LGPD.

O operador, no que lhe diz respeito, a lei considera ser responsável por processar dados pessoais em nome do controlador. Quem determina os termos do tratamento de dados é o controlador, e quem executa é o operador. Este segundo não pode controlar os dados, alterar a finalidade de seu uso nem mesmo seu uso. Ele limita seu trabalho ao processamento dos dados de acordo com as determinações e propósitos instituídos pelo controlador. De maneira oposta, o operador possui liberdade para decidir sobre o sistema, o método e as ferramentas que serão utilizadas na coleta dos dados e na forma com que serão armazenados. Sua principal responsabilidade é garantir a segurança desses dados, dos meios utilizados para transferi-los de uma organização para outra e das ferramentas aplicadas para recuperá-los.

Por fim, o encarregado pelo tratamento, conhecido na GDPR como *Data Protection Officer*, é responsável por receber reclamações e comunicações dos titulares dos dados, além de prestar os devidos esclarecimentos e garantir que sejam tomadas as medidas necessárias para o devido cumprimento das regras e das boas práticas de proteção de dados. Ademais, recebe comunicações da ANPD e deve adotar as providências que forem exigidas e orientar os funcionários sobre as práticas a serem tomadas. Apesar de não haver previsão legal, o

encarregado deve executar outras atribuições eventualmente determinadas pelo controlador ou estabelecidas em normas complementares. A LGPD não tratou de suas funções ou formação necessária para exercer o cargo.

Vale apontar algumas das várias atribuições e responsabilidades dos agentes de tratamento expostos acima presentes na LGPD, tais como: *(i)* observar os princípios gerais e a garantia dos direitos do titular (artigo 7º, §6º); *(ii)* obter consentimento, quando necessário (artigo 7°, §5°; artigo 8°, §6°); *(iii)* informar e prestar contas; *(iv)* garantir a portabilidade (artigo 9°; artigo 18; artigo 20); *(v)* garantir a transparência no tratamento de dados baseado em legítimo interesse (artigo 10, §2°); *(vi)* manter registro e manutenção das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse (artigo 37); *(vii)* elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, com observância dos segredos comercial e industrial (artigo 10; §3°; artigo 38); *(viii)* indicar o encarregado pelo tratamento de dados (artigo 41); *(ix)* reparar danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais (artigo 42 e 44, parágrafo único); *(x)* adotar medidas de segurança, técnicas e administrativas (artigo 46); *(xi)* garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término (artigo 47); *(xii)* comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (artigo 48); *(xiii)* salvaguardar os direitos dos titulares mediante a adoção de providências, como, por exemplo, a divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente (artigo 48, §2°); e *(xiv)* formular regras de boas práticas e de governança (artigo 50).

Dentre as atribuições e responsabilidades citadas, cabe destacar a aplicação do princípio da boa-fé, que deve ser como um guia aos agentes de tratamento de dados. Como um dos princípios fundamentais do direito privado, estabelece um padrão ético de conduta dos agentes de tratamento para com os titulares dos dados, acima de tudo em relação com os direitos correlatos, como cuidado em relação ao titular, respeito, informação sobre o conteúdo do negócio, probidade, colaboração e agir conforme a confiança depositada, com honestidade, de forma razoável e com equidade.

A predominância do princípio da boa-fé por parte dos agentes de tratamento é evidenciada em alguns dispositivos da LGPD, como: *(i)* o artigo 7º, §5: caso o controlador tenha que comunicar ou compartilhar dados pessoais já em tratamento, é necessário consentimento para tal fim, ressalvadas as exceções da lei; *(ii)* o artigo 8º, §5º: o consentimento para tratamento

dos dados poderá ser revogado pelo titular a qualquer tempo, devendo o controlador paralisar todo o tratamento previsto no artigo 5º, X; *(iii)* artigo 9º, §2º: uma vez já formalizado o consentimento inicial, caso a finalidade inicial do tratamento dos dados seja modificada, caberá ao controlador pedir autorização ao titular de dados; e *(iv)* o artigo 18º, VI: o titular de dados tem direito de obter do controlador a efetiva eliminação dos seus dados pessoais. Além disso, representam a necessidade de o titular dos dados confiar no controlador.

Os dispositivos citados acima, no entanto, são cabíveis exclusivamente ao controlador, e, eventualmente, ao operador. Isso representa a necessidade de os agentes de tratamento satisfazerem completamente a confiança depositada pelo titular dos dados em qualquer das referidas previsões. Destaca-se a situação de confiança plena do titular no controlador, principalmente, na eliminação de dados tratados em banco de dados eletrônico (artigo 18º, inciso VI). Isso porque não há como provar que os dados foram excluídos, tendo o titular apenas que confiar na afirmação do controlador. Por ser agente de dados que se encontra no mesmo grau de importância do controlador, ao operador é igualmente relevante o princípio da boa-fé.

Percebe-se, isto posto, que não há mais espaço para coleta e tratamento de dados pessoais sem finalidade relevante para o cidadão e, na maioria das vezes, sem consentimento, excluindo-se as exceções. É necessário que o cidadão se torne realmente dono de suas próprias informações e de seus dados, especialmente nas ocasiões em que o consentimento é necessário, de forma a evitar que o aceite não seja algo meramente proforma, ajustando o mercado a esse novo formato de tratamento de dados pessoais.

Dentre as atribuições e responsabilidades abordadas, cabe destacar a aplicação do princípio da boa-fé cabíveis exclusivamente ao controlador, e, eventualmente, ao operador. Além do mais, fica evidenciado que os dados pessoais podem ser tratados para atender aos interesses legítimos do controlador ou de terceiros, excetuando-se os casos em que prevalecem direitos e liberdades fundamentais do titular que exijam a proteção desses dados. Apesar de não haver definição de um limite claro por parte da legislação quando se envolve o tratamento de dados por legítimo interesse de terceiro, restam guardados os demais direitos do indivíduo.

3.1.4 O armazenamento de dados pessoais e o princípio da finalidade

Após o tratamento de dados, deve ser abordada a etapa do seu armazenamento. Com as evoluções dos cartões de memória, temos, hoje, a figura do "*cloud storage*" (armazenamento na nuvem), que possui a capacidade de acolher uma quantidade ilimitada de informações, sobre

bilhões de indivíduos. O armazenamento de dados envolve não apenas as informações presentes na rede mundial de computadores, mas também os bancos de dados. Anderson Schreiber explica:

> Entidades públicas e privadas valem-se com frequência cada vez maior de padronizações para avaliar a infinidade de casos individuais. Nesse cenário, os dados pessoais fornecidos de modo irrefletido ou capturados involuntariamente são usados na construção de "perfis", nos quais cada indivíduo acaba encaixando de acordo com características que o gestor das informações considera relevantes[62].

Desta forma, o armazenamento ou banco de dados se trata de informações pessoais arquivadas por entes públicos, privados ou pelo próprio indivíduo, com a finalidade de acesso futuro. Este armazenamento acaba por ameaçar direitos e garantias fundamentais, como a privacidade, a imagem e a honra, conforme visto no capítulo 2 deste trabalho.

Além disso, a Lei nº 13.709/2018, em seu artigo 5º, IV, conceitua banco de dados como um "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico".

De acordo com as subdivisões da LGPD, os dados estão divididos conforme abaixo:

> 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.

Essas subdivisões são primordiais para que seja assegurada a proteção, de forma mais eficaz, dos dados relativos às pessoas naturais, a fim de tutelar os direitos da personalidade. Neste momento, vale retomar o princípio da finalidade, que determina que todo e qualquer ato de utilização de dados pessoais deve ser informado ao seu titular. Márcio Cots e Ricardo Oliveira exemplificam bem no seguinte trecho:

> O tratamento de dados precisa ter uma finalidade, ou seja, um resultado único, específico e legítimo que deve ser alcançado com tal tratamento. O princípio serve não apenas para delimitar o objetivo final do tratamento, mas para tornar previsível o

[62] SCHREIBER, Anderson. Direitos da Personalidade. 3. ed. São Paulo: Atlas, 2014, p. 158.

> que dele se espera, inviabilizando tratamento posterior desvinculado com a finalidade original. Exemplos de violação ao princípio da finalidade: i) informar que a coleta de dados servirá para faturamento de produto ou serviço, mas utilizar os dados para campanhas de marketing; ii) informar que o compartilhamento de dados se dará com a empresa X, mas compartilhar os mesmos com a empresa Y, iii) informar que os dados não serão copiados, mas realizar cópias destes.[63]

O princípio em questão começou a ser utilizado no Brasil quando do uso do princípio da boa-fé objetiva, que buscava impor lealdade e transparência nas relações jurídicas. No entanto, as informações pessoais dos indivíduos eram divulgadas sem sua autorização, causando sérios constrangimentos e perdas monetárias, transpassando, de fato, seu direito à privacidade.

Fato é que é estabelecida uma relação de confiança entre o titular dos dados e o controlador, que possui elevado potencial de dano caso não seja realizado o devido tratamento. Se o titular autoriza a coleta, uso e tratamento dos seus dados, é porque há uma relação de confiança de que eles serão bem tratados, sem prejuízos, além da predominância do princípio da boa-fé por parte dos agentes de tratamento. Mas se o controlador utiliza esses dados, sem o consentimento do titular, sabendo ou com a finalidade de lhe causar prejuízo, mesmo que em sua defesa, essa seria uma violação aos direitos dos titulares. Ora, não é natural que alguém em sã consciência tome decisões esperando ser prejudicado por estas, ou seja, autorizar a coleta, uso e tratamento de seus dados se achar que será prejudicado.

No sentido da segurança e da proteção desses dados, conforme visto, a LGPD inovou ao determinar requisitos para que os agentes de tratamento possam armazenar os dados dos titulares, principalmente quanto à coleta e uso só poderem ser realizados havendo finalidade específica, comunicada ao titular e mediante expressa autorização dele. Outro avanço percebido foi a obrigação dos agentes de tratamento comunicarem aos titulares dos dados caso haja alguma violação de segurança destes dados, seja ela incidental ou ilícita, coibindo práticas reprováveis, como a propagação de informações pessoais sem o titular, muitas vezes, nunca sequer tomar conhecimento do fato.

Nessa perspectiva, o "Guia para a Lei Geral de Proteção de Dados", redigido pelo escritório de advocacia Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga, elucida:

> Os agentes de tratamento deverão proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração,

[63] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 77.

> comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais. Para tanto, deverão adotar uma série de medidas de segurança, técnicas e administrativas.[64]

Em consonância com o trecho destacado, se os agentes de tratamento não cumprirem seu dever de proteção dos dados, cabe à ANPD aplicar sanções administrativas aos mesmos. Nos casos das multas aplicadas às empresas, o montante arrecadado é inteiramente destinado aos cofres do Estado, não sendo convertidos em indenização para os verdadeiros prejudicados: os titulares dos dados compartilhados. A LGPD traz um viés pedagógico e punitivo, e, no entanto, deixa de lado o indenizatório.

Por fim, considerando que a ANPD acumula grande parte das funções de fiscalizar, investigar e garantir a segurança do disposto na lei, deve haver o quanto antes a estruturação desse órgão para garantir a eficácia prática da LGPD.

Percebe-se, desta maneira, a necessidade de cumprir com o princípio da finalidade, devendo todo e qualquer ato de utilização de dados pessoais ser informado ao seu titular. Soma-se a isso a obrigatoriedade de os agentes de tratamento comunicarem aos titulares dos dados caso haja alguma violação de segurança. A seguir, será tratada a última etapa relacionada à proteção de dados pessoais: a eliminação.

3.1.5 A eliminação dos dados pessoais

Outro importante direito no contexto atual de mundo cada vez mais virtual é o da eliminação de dados, a fim de examinar os reflexos nos direitos da personalidade. Isso porque os danos causados pelo mau uso ou armazenamento dos dados podem tomar patamares muito elevados, como expõem Cristiano Chaves, Nelson Rosenvald e Felipe Braga Netto:

> Dizer que os danos aumentaram em nosso século envolve certo truísmo. Se nós, no início do século passado, engatinhávamos nas possibilidades tecnológicas, se sequer conhecíamos a televisão ou o avião, se uma notícia demorava lentos meses para partir da Europa e chegar até aqui, hoje, desnecessário dizê-lo, a situação modificou-se de modo impensável. É possível até afirmar, sem medo de errar: talvez a mais otimista das previsões não previsse que chegaríamos aonde chegamos, em possibilidades tecnológicas. As possibilidades de danos são muitas. Algumas perfazem crime, como

[64] MATTOS FILHO, VEIGA FILHO, MARREY JR. E QUIROGA ADVOGADOS. Guia para a Lei Geral de Proteção de Dados. São Paulo. 2018. Disponível em: https://publicacoes.mattosfilho.com.br/books/bdtv/#p=1. Acesso em: janeiro de 2021. p. 25.

> o uso de dados de cartões de crédito ou débito de forma indevida ou sem autorização. Da mesma forma, a invasão não autorizada para furtar informações confidenciais.[65]

Dito isso, entende-se a necessidade de realização de uma eficaz eliminação de dados. O Marco Civil da Internet, em seu artigo 7º, inciso X já previa a eliminação de dados e, agora, a LGPD a regulamentou, assegurando a faculdade do titular dos dados de solicitá-la ao agente controlador. Além disso, o artigo 16 da LGPD também prevê a obrigatoriedade de o controlador excluir os dados pessoais após o término do tratamento.

No entanto, esse não é um direito absoluto, visto que no próprio artigo 16 a LGPD elenca um rol taxativo de hipóteses em que não há obrigatoriedade de eliminação dos dados pelo controlador, mesmo com solicitação do titular, conforme abaixo:

> 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.

Analisando a questão, é possível perceber o impacto que o direito de eliminar os dados pessoais pode causar, sobre a atividade econômica desempenhada pelos agentes de tratamento e os direitos fundamentais dos envolvidos. Inicialmente, é preciso reconhecer que o armazenamento de dados pessoais é um dos pilares da atividade econômica empresarial já que é uma importante fonte de ativos. Justamente por isso que muitas empresas escolhem descumprir a lei, negando a eliminação dos dados. O valor das informações pessoais é tão alto que é preferível arcar com as possíveis sanções decorrentes de tal conduta.

Uma pesquisa realizada pela Talend sobre a análise da implementação da GDPR aponta que após 25 meses de *vacatio legis* e 3 meses da entrada em vigor da lei, totalizando 28 meses para as empresas se adequarem à legislação, 70% delas ainda não estavam cumprindo suas determinações. Um dos principais descumprimentos se dá pela negativa em eliminar dados pessoais arquivados. Mesmo se expondo às eventuais sanções legais, vale destacar outra consequência dessa atitude: a perda da respeitabilidade das empresas frente ao mercado e à

[65] FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. Curso de Direito Civil: Responsabilidade Civil. 5. ed. Salvador: Juspodivm, 2018, p. 771.

consequente reputação.

Ademais, essa conduta pode acabar sendo corroborada, mesmo que indiretamente, pelo próprio Poder Judiciário, como se percebe na decisão proferida pelo magistrado da 2ª Vara do Juizado Especial Cível de São José dos Campos, que negou pedido de usuário do PagSeguro de ter seus dados eliminados do sistema da companhia, sob a arguição de que esta não havia manipulado tais dados de forma indevida. Apesar de a sentença ter sido reformada pelo Tribunal de Justiça de São Paulo, o fato de a primeira instância ter adotado tal entendimento contrariando o Marco Civil da Internet, mostra o eventual despreparo dos juristas brasileiros para lidar com situações atuais tão relevantes que podem acabar causando grande impacto aos brasileiros.

Em segundo lugar, no âmbito dos direitos fundamentais e de personalidade, nunca houve tanta valorização do direito à privacidade. Os dados nunca foram coletados tão rapidamente, também, sem que o titular saiba o que será feito com seus dados, bem como aumentando a possibilidade de ataques *ciber*criminosos, por exemplo. Exemplificando, houve dois casos emblemáticos recentes de vazamento de dados: *(i)* os usuários do Facebook, somando o vazamento de 87 milhões de usuários; e *(ii)* o vazamento de dados pessoais de 223 milhões de brasileiros, de origem ainda desconhecida e em investigação pelas autoridades. Os impactos desses vazamentos são os mais diversos, desde veiculação de marketing a clonagem de cartão, uso dos dados para realizar saques indevidos do FGTS e outros golpes.

Muitas vezes tem sido sobreposta a segurança digital à física ou patrimonial, ao passo que as pessoas saem sem se preocupar em trancar a porta de casa, mas não deixam o computador ou o celular desbloqueado ao se ausentar. Silvado Pereira, coordenador do centro de Estudos em Comunicação, Política e Tecnologia (CTPol) da Universidade de Brasília, ratifica tal pensamento ao afirmar que "privacidade envolve, na verdade, autonomia e liberdade. Quanto menos privacidade você tiver, menos liberdade e autonomia terá". Em relação ao direito ao esquecimento, é assegurado ao titular o direito de não permanecer vinculado a informações inverídicas, incompletas ou que se tornem irrelevantes, estando intimamente ligado ao direito de exclusão de dados.

Conforme exposto, não há dúvidas quanto à necessidade de tutela da privacidade em relação aos dados. Esse movimento tem se tornado uma tendência mundial, e pode ser confirmado pela decisão do Tribunal de Justiça da União Europeia ao condenar o Google a apagar dos resultados de buscas links associados a pessoas dependendo da natureza da informação e da gravidade para a vida privada.

Justamente pelo impacto que o não cumprimento do direito de eliminar os dados

pessoais pode causar sobre a atividade econômica desempenhada pelos agentes de tratamento e os direitos fundamentais dos envolvidos, é percebida a necessidade de assegurar ao titular dos dados o direito de não permanecer vinculado a informações inverídicas, incompletas ou que se tornem irrelevantes, que está intimamente ligado ao direito de exclusão de dados.

Dessa forma, resumidamente, fica evidente que devem ser observadas as etapas de proteção de dados, levando-se em conta: *(i)* sua natureza, que definirá o grau de proteção a ser dado; *(ii)* a coleta e armazenamento apenas dos dados que forem essenciais para a segurança e/ou gestão da empresa; *(iii)* o princípio da finalidade, que determina que todo e qualquer ato de utilização de dados pessoais deve ser informado ao seu titular; e *(iv)* a eliminação eficaz dos dados após o término do seu uso.

Em seguida, será exposta a responsabilidade civil prevista na LGPD nos casos de não cumprimento dos seus dispositivos, incluindo o posicionamento judicial sobre o tema – mesmo que ainda escasso, de forma a evidenciar a incipiente aplicação das diretrizes da LGPD nos casos concretos.

3.2 A RESPONSABILIDADE CIVIL NA LGPD

A priori, vale rememorar alguns conceitos tratados no capítulo anterior, como titular, controlador, operador e encarregado dos dados pessoais. Márcio Cots e Ricardo Oliveira ilustram bem os papéis desenvolvidos pelos agentes:

> Vamos utilizar um exemplo prático: um site de comércio eletrônico. A Empresa X, fabricante de artigos esportivos, deseja ter um site para venda de seus produtos diretamente aos consumidores, mas, como o comércio virtual não é sua atividade principal, deseja delegar algumas atividades do negócio a alguns prestadores de serviço. Assim, contrata uma plataforma virtual completa com a empresa A, a gestão e meio de pagamento com a empresa B, a gestão e logística com a empresa C e a gestão do marketing e propaganda com a empresa D. Ao receber um pedido, os dados pessoais do usuário são captados pela plataforma (empresa A), depois segue para o meio de pagamento (empresa B) ao mesmo tempo que é incorporada ao banco de dados da empresa Y. Após, os dados pessoais seguem para a empresa D, com a determinação que realize a entrega do produto, ao mesmo tempo em que são encaminhados à empresa. E, para inclusão no mailing e demais atividades de divulgação. Todas as empresas do arranjo mencionado terão acesso aos dados do usuário do site, mas apenas a empresa X se encaixa na figura de controlador. As demais seguem as orientações da empresa X para concretizar os pedidos e entregar o produto, não decidindo, por si, o que será feito dos dados recebidos, nem o que será feito posteriormente com eles. Assim, as empresas A, B, C e D são operadoras. Em suma, o controlador toma as decisões do tratamento, os operadores seguem as

> orientações do controlador, cumprindo uma função específica no processo de tratamento. [66]

Como visto, o controlador e o operador são tidos como agentes de tratamento de dados pessoais e assumem algumas obrigações, dispostas no artigo 37 da LGPD, para que possam manejar os dados pessoais. Dentre elas, cabe a eles manter o devido registro das operações de tratamento de dados pessoais realizadas, principalmente quando envolver o legítimo interesse. No artigo seguinte da lei, está disposto que, caso necessário, a autoridade nacional poderá pedir relatório de impacto da proteção de dados, conforme abaixo:

> 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.

Conforme o dispositivo acima destacado, cabe destacar que não se trata de um rol exaustivo, apenas exemplificativo das informações que o relatório deve conter. Dessa forma, o relatório de impacto deverá conter essencialmente essas informações, sem que sejam restritas a elas.

Neste momento, vale tratar do regime jurídico da responsabilidade civil na LGPD. Em seu artigo 42, a lei define que: "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". Esse dispositivo é respaldado em regras elementares de responsabilidade civil, a saber: o *caput* do art. 927 do Código Civil, estabelecendo que "aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

Isto posto, a conduta que obrigaria à reparação é a ofensa aos termos da legislação em questão, como Márcio Cots e Ricardo Oliveira demonstram, "o nexo causal do dano está intrinsecamente ligado à violação LGPD, sendo que, se não houve violação, não se torna

[66] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 165.

aplicável o art. 42, não se configurando ato ilícito".[67] Além disso, é prevista responsabilidade solidária do operador e do controlador, conforme o trecho abaixo do artigo 42 da LGPD:

> § 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.

Conforme já exposto, além do controlador, o operador também pode ter acesso aos dados do titular, também sendo obrigado a indenizá-lo no caso de danos. Soma-se à isso a inversão do ônus da prova prevista no artigo 373 do Código de Processo Civil e no artigo 42 da LGPD: "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". Isso ocorre para que seja assegurada a inviolabilidade dos direitos do titular dos dados, assim como é feito com os consumidores, tendo essa exceção.

No entanto, há hipóteses em que os agentes de tratamento não serão responsabilizados civilmente, conforme o artigo 43 da LGPD, quais sejam: *(i)* se provar não ter realizado o tratamento dos dados; *(ii)* se o dano decorrer de culpa exclusiva do titular ou de terceiros; e *(iii)* se não tiver havido violação aos termos da LGPD. Essas são as causas excludentes de responsabilidade aplicáveis à matéria definidas pela própria lei, devendo, então, os agentes de tratamento responder objetivamente pelos danos causados, sem que haja verificação de culpa ou dolo.

É importante destacar que não há regra específica na LGPD que disponha sobre a responsabilização do encarregado pelos dados. Nesse sentido, Márcio Cots e Ricardo Oliveira sugerem que o encarregado não responde perante o titular ou o agente nacional quanto ao tratamento de dados realizados pelo controlador, já que "é este último que concentra todo o poder decisório sobre o tratamento de dados, atuando o encarregado, apenas como comunicador de tais decisões aos terceiros interessados". Ainda assim, segundo os autores, "o encarregado não estará isento de responder por seus atos perante o controlador ou, na esfera penal, perante

[67] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 175.

o controlador ou os terceiros interessados, em decorrência da execução de suas atribuições". [68] Isso ocorre já que o encarregado pode agir de má-fé e prejudicar o titular, mesmo o poder decisório estando nas mãos do controlador.

Então, as sanções administrativas previstas na LGPD são:

> 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:
> 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;
> § 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.

Sendo assim, podem ser aplicadas mais de uma sanção, limitadas a 50 milhões de reais para cada ato infracional. Até porque pode haver cumulação de sanções administrativas com a responsabilidade civil, a fim de que os danos causados aos titulares sejam reparados. Além disso, conforme apontam Cristiano Chaves, Nelson Rosenvald e Felipe Braga Netto, o instituto da responsabilidade civil possui funções plurais, quais sejam:

> Cremos que no Direito Brasileiro do alvorecer do século XXI a conjunção destas orientações permite o estabelecimento de três funções para a responsabilidade civil: (1) função reparatória: a clássica função de transferência dos danos do patrimônio do lesante ao lesado como forma de reequilíbrio patrimonial; (2) função punitiva: sanção consistente na aplicação de uma pena civil ao ofensor como forma de desestímulo de

[68] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 171.

> comportamento reprováveis; (3) função precaucional: possui o objetivo de inibir atividades potencialmente danosas.[69]

Percebe-se, então, que tais funções, no sistema judicial brasileiro, não são devidamente empregadas na maioria dos casos. É normal que o valor da indenização seja inferior em relação ao dano causado. Diante do exposto, nota-se, no entanto, que houve notável avanço em relação às sanções administrativas com a previsão de critérios para emprego de penalidades.

Apesar das sanções previstas, há hipóteses em que os agentes de tratamento não serão civilmente responsabilizados, sendo um dos motivos principais a observância do disposto na LGPD. Sendo assim, a seguir, serão analisados posicionamentos judiciais quanto à responsabilidade civil pela má gestão de dados pessoais (3.2.1) e as sanções aplicáveis pela ANPD nesses casos (3.2.2).

3.2.1 Posicionamento jurisprudencial quanto à responsabilidade civil pela má gestão de dados pessoais

Pela recente percepção da importância da proteção de dados, vê-se poucas jurisprudências sobre o tema até o momento. No entanto, certo é que, em breve, haverá muito conteúdo relacionado a isso. Percebe-se que o judiciário brasileiro, relativamente à matéria, tende a impor a coleta e/ou tratamento de dados indevidos como condição para caracterização de danos morais quando houver causado prejuízo à vítima. Seguem, abaixo, dois julgados do TJRS que confirmam a assertiva:

> APELAÇÃO CÍVEL. PROCOB. AÇÃO DE INDENIZAÇÃO. COMERCIALIZAÇÃO DE INFORMAÇÕES PESSOAIS DE CONSUMIDORES. DANO MORAL NÃO CONFIGURADO. ARQUIVO DE CONSUMO. INEXISTÊNCIA DE ILEGALIDADE. AUSÊNCIA DE PROVA DO PREJUÍZO AO CONSUMIDOR. A elaboração, organização, consulta e manutenção de bancos de dados sobre consumidores não é proibida pelo Código de Defesa do Consumidor; ao contrário, é regulada por este. Hipótese em que o serviço colocado à disposição das empresas conveniadas pela ré não se reveste de ilegalidade, considerando que as informações expostas não são consideradas de caráter sigiloso ou íntimo, mas de fácil e ampla circulação no mercado de consumo, para proteção do crédito e segurança nas relações comerciais. Ausência de violação à vida privada, imagem ou intimidade. Inexistência, ainda, de provas de que a divulgação de dados pela requerida tenha causado qualquer prejuízo à parte autora, ônus que lhe incumbia, não havendo como

[69] FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. Curso de Direito Civil: Responsabilidade Civil. 5. ed. Salvador: Juspodivm, 2018, p. 62.

> se conceder indenização por dano hipotético. Sentença de improcedência confirmada.[70]

> APELAÇÃO CÍVEL DESPROVIDA.14 APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. COMERCIALIZAÇÃO DE DADOS DE CONSUMIDORES. PROCOB. VIOLAÇÃO AOS DIREITOS DE PRIVACIDADE E INTIMIDADE. NÃO CARACTERIZADO. DANO MORAL. INOCORRÊNCIA. Trata-se de ação indenizatória, através da qual a parte autora postula o pagamento de indenização por danos morais, em razão da disponibilização de seus dados pessoais pela requerida, julgada improcedente na origem. O sistema mantido pela requerida enquadra-se no conceito de arquivo de consumo, visto que reúne informações acerca dos consumidores, tais como nome, CPF, telefones e endereços, fornecendo-os aos clientes, mediante contrato de prestação de serviços. Serviços prestados pela demandada que não se caracterizam como ilícito, especialmente por coletar dados do consumidor disponíveis no mercado, não se tratando de dados sigilosos. O conjunto fático-probatório não foi apto a atestar que o ora recorrente sofreu dano à imagem ou a sua esfera psíquica, razão pela qual o apelante não se desincumbiu do ônus que lhe recaia, ex vi legis do artigo 373, I, do CPC, uma vez que a mera alegação não gera, por si só, o dever de indenizar. Desta feita, imperiosa a manutenção sentença, haja vista que está de acordo com a orientação deste colendo tribunal de... justiça, bem como está bem fundamentada, rente aos fatos deduzidos na origem. APELAÇÃO DESPROVIDA.[71]

Vê-se uma concepção materialista sobre o tema ao caracterizar a responsabilidade civil apenas no caso quanto a coleta e/ou tratamento dos dados, ainda que realizados indevidamente e que tenham causado prejuízo concreto às vítimas. Nos casos em tela, foi desconsiderada a própria conduta ilícita da empresa que manteve informações que não deveria em sua base de dados.

Em outros casos, a jurisprudência reconhece que a conduta da empresa foi ilícita, mas descaracteriza o dano e o dever de indenizar ao afastar a responsabilidade civil, entendendo não ter havido prejuízo concreto à vítima, conforme o julgado abaixo:

> APELAÇÃO CÍVEL. COBRANÇA INDEVIDA. CONTRATO DE SERVIÇOS DE TELEFONIA MÓVEL DESCONHECIDO PELO AUTOR. AUSÊNCIA DE DANO MORAL. MERO ABORRECIMENTO. Ação declaratória de inexistência de débito c/c indenizatória movida em face da ré, através da qual o autor sustenta que foi surpreendido com uma ligação de prepostos da ré informando-lhe sobre a existência de dívida referente a uma linha telefônica. Conforme se observa dos autos, o demandante foi vítima de uma fraude envolvendo os seus dados pessoais, tendo a ré efetuado cobrança indevida decorrentes da contratação, por terceiro, de uma linha telefônica móvel. Na hipótese dos autos observa-se com clareza que a conduta da ré, embora reprovável, não repercutiu na esfera dos direitos da personalidade do demandante, vez que não houve inclusão do seu nome no rol de maus pagadores ou cobrança vexatória ou humilhante. Desse modo, tenho que não está demonstrado

[70] TJRS. 18ª Câmara Cível, Apelação Cível nº 70069154854, Relator Túlio de Oliveira Martins, j. 30/06/2016, DJE: 08/07/2016.
[71] TJRS, 6ª Câmara Cível, Apelação Cível nº 70077938512, Relator Niwton Carpes da Silva, j. 30/08/2018, DJE: 12/09/2018.

> qualquer prejuízo de grande monta ao apelado, resumindo-se a situação narrada a mero aborrecimento que não configura dano moral, nos termos do enunciado 75/TJERJ. No que tange à verba honorária, não há motivo para majorá-la, na medida em que o montante fixado atendeu aos critérios estipulados pelos incisos do § 2º, do art. 85, do CPC. Desprovimento do recurso.[72]

Nesse julgado é reconhecido que a empresa ré agiu culposamente ao permitir que terceiro acessasse aos dados de seu usuário e, no entanto, afirmou-se que não houve dano à vítima, afastando a responsabilidade civil da empresa. Cumpre destacar que extrapola em muito o mero dissabor cotidiano o fato de a empresa, ainda que não tenha sido dolosamente, tenha permitido acesso a informações pessoais, privativas e íntimas de um dos seus usuários a terceiro. Conforme o exposto até o momento, para caracterizar o ilícito e o dano, basta a omissão culposa da empresa e o fato do acesso indevido aos dados pessoais do indivíduo.

Nos casos em que o judiciário reconhece o dano causado à vítima pela coleta e tratamento indevidos de dados pessoais, caracterizando a responsabilidade civil, a indenização fixada é ínfima em relação ao dano experimentado, conforme pode ser observado abaixo:

> Apelações Cíveis. Responsabilidade Civil. Alegação de prejuízo material e moral decorrente de uso dos dados pessoais. Sentença que condena a ré em danos morais no valor de R$ 5.000,00. Apelação de ambas as partes. O autor com pretensão de reforma para que sejam acolhidos todos os pedidos iniciais, já que restou comprovado o ato ilícito e sucumbência total da ré. A ré para que seja afastada a condenação em danos morais. Incontroverso o uso dos dados do autor pela ré que, inclusive, foi por esta confessado. Ocorrência de ato ilícito e violação da intimidade. Danos morais configurados. Valor fixado em R$ 5.000,00 que não merece reparo, eis que atende aos princípios da razoabilidade e proporcionalidade, e não enseja enriquecimento sem causa. Ausência de intenção deliberada em prejudicar o autor. Falta de cautela na vinculação do número do PIS. Dano material não comprovado. Ausência de cobrança de dívidas decorrentes do ato praticado pela ré. Honorários Advocatícios fixados conforme art. 85, § 2º do CPC. Recursos desprovidos.[73]

> APELAÇÃO CÍVEL – Interposição contra sentença que julgou procedente ação indenizatória por danos morais. Dados cadastrais pessoais expostos em site da internet. Violação ao direito constitucional à privacidade. Dano moral caracterizado. Indenização bem sopesada em R$ 5.000,00 (cinco mil reais). Litigância de má-fé afastada. Sentença mantida.[74]

Depreende-se, pelo exposto, que a jurisprudência brasileira tem descaracterizado o dano decorrente da má gestão dos dados pessoais arguindo não haver prejuízo coletivo, ao passo que

[72] TJRJ, 15ª Câmara Cível, Apelação Cível nº 0015005-34.2017.8.19.0011, Relator Ricardo Rodrigues Cardozo, j. 18/07/2019, DJE: 18/07/2019.
[73] TJRJ, 26ª Câmara Cível, Apelação Cível nº 0393241-25.2015.8.19.0001, Relatora Natacha Nascimento Gomes Tostes Gonçalves de Oliveira, j. 22/11/2018, DJ: 22/11/2018.
[74] TJSP, 33ª Câmara de Direito Privado, Apelação Cível 4007792-98.2013.8.26.0577, Relator: Mario A. Silveira, j. 30/11/2015, DJE 01/12/2015.

reduziu a indenização nos casos em que foi reconhecido o dano e caracterizada a responsabilidade civil, acreditando dever agir de tal forma para evitar o enriquecimento sem causa do titular dos dados.

Contrariamente do verificado no teor dos julgados colacionados, cumpre defender que a coleta e o tratamento indevido de dados pessoais deve ser um fator que caracteriza um autêntico dano, não sendo necessária a comprovação de um prejuízo concreto para ser caracterizada a responsabilidade civil. O fato de uma empresa permitir, ainda que culposamente, que terceiro, estranho e desconhecido, tenha acesso a informações pessoais, privadas e/ou íntimas caracteriza um dano, correspondente à violação à privacidade e, em alguns casos, da intimidade dos indivíduos lesados.

Por todo o exposto é que se faz necessário estudar e expor claramente quais são os requisitos e os trâmites que devem ser cumpridos, em cumprimento à LGPD, para que sejam realizadas investigações internas dos programas de *compliance* e celebrados acordos de cooperação com a administração pública, conforme será feito no próximo capítulo. Principalmente para proteger a privacidade, a intimidade e os dados pessoais dos indivíduos envolvidos, bem como sejam observados os princípios de segurança, confidencialidade e integridade dos dados armazenados, de acordo com o exposto ao longo da pesquisa.

Após tratar das etapas para proteção dos dados pessoais, foi tratada a responsabilidade civil na LGPD, bem como o posicionamento judicial quanto à má gestão de dados pessoais. A seguir, complementarmente, serão abordadas informações relativas à autoridade Nacional de Proteção de Dados (ANPD) e as possíveis sanções a serem aplicadas por ela no caso de não cumprimento do disposto na legislação.

3.2.2 A Autoridade Nacional de Proteção de Dados (ANPD) as sanções aplicáveis

A ANPD foi criada após edição da Lei Federal n.º 13.853/2019, oriunda da conversão da Medida Provisória nº 869/2018. No artigo 55 da LGPD é conceituada a autoridade em referência como sendo um órgão integrante da administração pública que faz parte da estrutura da Presidência da República, com autonomia técnica. Sua necessidade se deu, justamente, pela regulamentação da proteção de dados e os impactos decorrentes dela em todos os âmbitos da sociedade.

A tarefa da ANPD é orientar, através de seu corpo técnico especializado, todos os agentes da sociedade sobre quais os limites da LGPD, especificando, de forma prática, como

deve se dar a concretização dos conceitos que permeiam o texto legal. Ademais, deve cooperar com as autoridades de controle e proteção de dados de outros estados, dando enfoque à defesa e exercício dos direitos das pessoas residentes no exterior.

A compreensão da evolução histórica e normativa da atuação da ANPD envolve a análise realizada no início do trabalho sobre os demais diplomas legais que culminaram na LGPD. Cabe destacar que a agência é um mecanismo de atuação da LGPD, cuja principal função é zelar pela proteção de dados pessoais por meio de competência normativa, deliberativa, fiscalizadora e sancionatória.

Para isso, as competências mais relevantes estão dispostas no artigo 55 da LGPD, quais sejam: *(i)* editar normas e procedimentos sobre a proteção de dados pessoais (inciso II); *(ii)* deliberar sobre a interpretação da LGPD, suas competências e os casos omissos (inciso III); *(iii)* requisitar informações aos controladores e operadores de dados pessoais (inciso IV); *(iv)* implementar mecanismos para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a Lei (inciso V); *(v)* fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo (inciso VI); e *(vi)* comunicar às autoridades competentes as infrações penais das quais tiver conhecimento (inciso VII).

A agência, portanto, possui nível superior de competência técnica, estando bem posicionada para decidir sobre qual o melhor sentido do texto normativo e quais fatores representam ameaças reais ao cumprimento da lei. Além disso, para exercer seu poder de regulamentar, deve se sujeitar ao artigo 37 da Constituição Federal, devendo obedecer aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. No entanto, para evitar que haja uma profunda regulamentação e intervenção na atividade econômica, §1º do artigo 55-J da LGPD dispõe que a atividade deve ocorrer com a mínima intervenção.

Dessa forma, a principal habilidade da ANPD é empregar padrões de ação que facilitem o cumprimento das normas e mantenham o espírito da lei, diante das peculiaridades de cada tecnologia. Ela se utiliza de dois mecanismos da LGPD de proteção aos dados pessoais: a responsabilização administrativa por meio de sanções aplicadas pela ANPD (a multa aplicada às empresas pode chegar a 2% de seu faturamento anual, limitado tal patamar a até R$ 50 milhões por infração) e a responsabilização civil e ressarcimento de danos, por meio de ação do poder judiciário.

O tratamento de dados pessoais deve observar os princípios expostos no artigo 6º da LGPD já citados no capítulo 2. O não cumprimento de uma das 10 bases legais evidenciadas o

artigo 7º da GPD pode resultar em sanções administrativas (artigo 52 da LGPD) a serem aplicadas pela ANPD aos agentes envolvidos, gradativa, isolada ou cumulativamente, quais sejam: *(i)* multas de até R$ 50 milhões; *(ii)* publicização da infração; *(iii)* bloqueio e eliminação de dados pessoais; e *(iv)* suspensão de banco de dados e proibição do exercício de atividades de tratamento de dados.

As aplicações de sanções são de competência exclusiva da ANPD, como a LGPD deixou claro, após procedimento administrativo e sendo assegurada a ampla defesa. Eventuais ilicitudes cometidas no âmbito de tratamento de dados serão objeto de fiscalização e punição pela ANPD e, não, pelo órgão que esteja envolvido. Isso impacta diretamente na relação que a Autoridade possui com os demais órgãos sancionadores do poder público.

Assim, o processo administrativo se torna indispensável na apuração de ato infracional. O processo sancionador ao acusado se dará conforme os princípios elencados na Constituição Federal, como o devido processo legal, o princípio da presunção de inocência, o direito à ampla defesa e ao contraditório, o princípio da decisão motivada e o instituto da prescrição, que constam no rol de direitos e garantias constitucionais de forma positivada e que deve ser garantido na atuação da Agência. Esses direitos fundamentais, além de serem democráticos e individuais, possuem eficácia e aplicabilidade imediata. Também se aplica o princípio da não autoincriminação e do direito ao silêncio, verificados no artigo 5º da lei, pois o réu tem o direito de não se expressar em juízo ou fora dele, de forma a evitar sua autoincriminação.

Da mesma maneira, o direito de defesa é tido como uma medida de participação na tomada de decisões administrativas. A garantia do direito de defesa está intimamente ligada a uma pretensão repressiva e é considerada um pressuposto de eficácia do procedimento administrativo[75]. É por meio do contraditório que serão construídos novos significados normativos que sejam compatíveis com os casos concretos perante a Agência.

Já o direito de defesa se apresenta de outras formas. A administração pública tem o dever de ouvir o administrado antes de tomar uma decisão que o afete. Por isso, há a necessidade de uma audiência prévia, com a finalidade de boa administração e de garantia do indivíduo. Posto isso, o princípio que rege não é apenas de justiça, mas também de eficácia[76]. Este princípio ganha espaço justamente pela necessidade do Estado tutelar o bem-estar dos cidadãos e atender às classes menos favorecidas da sociedade.

---

[75] FERREIRA, Luiz Alexandre Cruz. O direito de defesa na concepção dos atos administrativos. Revista jurídica, [s.l.], 2012. Disponível em: https://www.uniaraxa.edu.br/ojs/index.php/juridica/article/viewFile/84/76. Acesso em: janeiro de 2021.
[76] Ibidem.

Resumidamente, diante do exposto, as principais sanções e/ou advertências que pode ser aplicadas pela ANPD nos casos de descumprimento do disposto na LGPD são: *(i)* advertências com indicação de prazos para adoção de medidas corretivas; *(ii)* multa simples de até 2% do faturamento da empresa no seu último exercício - excluindo os tributos - e limitada até o valor de R$ 50.000.000,00 por infração; *(iii)* multa diária, observando o limite anterior; *(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; e *(vi)* eliminação dos dados pessoais a que se refere infração.

4 O USO DAS INFORMAÇÕES COLETADAS NAS INVESTIGAÇÕES INTERNAS NA CELEBRAÇÃO DE ACORDOS COM A ADMINISTRAÇÃO PÚBLICA EM CONFORMIDADE COM A LGPD

Após expor as etapas de proteção de dados pessoais, incluindo como deve ser o processo de coleta, uso, tratamento, armazenamento e eliminação dos dados pelas empresas, bem como a responsabilidade civil decorrente do não cumprimento das diretrizes da LGPD, faz-se necessário elencar os requisitos necessários para uso de dados pessoais oriundos de investigações internas nos acordos de cooperação com a administração pública.

Para isso, inicialmente serão especificados os tipos de acordo, bem como as justificativas e os pilares dos programas de leniência (4.1). Em um segundo momento, serão abordados os requisitos de celebração destes acordos (4.2), inclusive o legítimo interesse do controlador no uso dos dados coletados (4.2.1), o consentimento (4.2.2) e as condições particulares de diferentes hierarquias de funcionários (4.2.3).

4.1 CONDIÇÕES PARA REALIZAÇÃO DE ACORDOS COM A ADMINISTRAÇÃO PÚBLICA

Consoante o exposto no capítulo 2, foram abordados os aspectos gerais dos acordos de cooperação que podem ser celebrados com a administração pública, bem como seus requisitos (4.1.1), quais sejam: *(i)* Leniência Antitruste (4.1.1.1); *(ii)* Leniência no Sistema Financeiro Nacional (4.1.1.2); *(iii)* Leniência Anticorrupção (4.1.1.3); e *(iv)* Leniência do Ministério Público (4.1.1.4). Sendo assim, neste capítulo, serão abordados as especificidades e os tipos de acordo existentes.

4.1.1 Tipos de acordos de cooperação com a administração pública

Serão tratados, no âmbito dos acordos de leniência, os seguintes acordos: *(i)* Acordo de Leniência Antitruste – artigos. 86 e 87 da Lei nº 12.529/2011; *(ii)* Acordo de Leniência no âmbito do Sistema Financeiro Nacional (BCB e CVM) - artigo 30 e seguintes da Lei nº 13.506/2017; *(iii)* Acordo de Leniência Anticorrupção - artigos. 16 e 17 da Lei nº 12.846/2013; *(iv)* Acordo de Leniência do Ministério Público (MP) - artigo 129, I da CF/88, artigo 5º e 6º da Lei 7.347/85, artigo 26, da Convenção de Palermo, artigo 37 da Convenção de Mérida, artigo

3º, §2º e 3º do CPC, artigo 840 e 932, III, do CC/02, artigo 16 a 21 da Lei 12.846/2013, Lei nº 13.410/2015, princípio da eficiência, art. 37. *caput* da CF/88; *(v)* Acordo de Supervisão do Bacen; e *(vi)* Acordo de Supervisão da CVM.

Já no que tange aos termos de compromisso, serão abordados: *(i)* Termo de Compromisso de Cessação do CADE; *(ii)* Termo de Compromisso do BCB; e *(iii)* Termo de Compromisso da CVM. Além desses, serão abordadas as demais possibilidades de acordo, tais como o termo de ajustamento de conduta em matéria trabalhista e ambiental. Também serão abordadas outras formas de acordo, como os de não persecução criminal.

Frente a multiplicidade de Programas de Leniência no Brasil e dos acordos que podem ser celebrados com a administração pública, é necessário abordar suas especificidades técnicas e práticas a fim de que não reste dúvidas sobre os contornos jurídicos de cada instituto[77]. Para melhor compreensão, os acordos de leniência serão divididos em 4 grupos: Leniência Antitruste, no Sistema Financeiro Nacional, Anticorrupção e do MP, conforme será feito a seguir.

4.1.1.1 Leniência Antitruste

O acordo de leniência da Lei nº 12.529/2011 pode ser celebrado por empresas, pessoas físicas ou ambos, separadamente ou em conjunto, que estejam envolvidas em prática anticoncorrencial coletiva, ou seja, que cometerem infrações contra a ordem econômica. No caso do proponente ser uma empresa, os benefícios do acordo podem se estender aos seus colaboradores antigos e atuais, até a outras empresas de um mesmo grupo econômico envolvidas na infração, desde que haja cooperação com as investigações e que o acordo seja assinado em conjunto com a proponente[78].

Os colaboradores que não aderirem ao acordo no mesmo momento da empresa ainda possuem a possibilidade de aderir posteriormente mediante avaliação de conveniência do Cade, autarquia federal brasileira vinculada ao Ministério da Justiça e Segurança Pública, que compõe o Sistema Brasileiro de Defesa da Concorrência ao lado da Secretaria de Acompanhamento Econômico. De maneira oposta, se o proponente do acordo for uma pessoa física e a empresa não o celebrar em conjunto, não poderá se aproveitar dos benefícios depois. Isso ocorre para

[77] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 26.
[78] Deloitte. Orientações para celebração de acordos de cooperação por empresas. IBDEE, agosto de 2018. Pesquisa "Acordos de Cooperação – Percepção do Empresariado sobre o Tema e Práticas Adotadas", p. 9.

aumentar a instabilidade do cartel ao passo que incentiva que os envolvidos em atos ilícitos denunciem a prática anticompetitiva o quanto antes. Agora, após evoluções da lei em questão, até mesmo o líder do cartel pode propor um acordo de leniência[79].

Alguns de seus benefícios são, no caso da leniência total, a imunidade administrativa total, e no caso da leniência parcial, a redução da penalidade aplicável de 1/3 a 2/3. Criminalmente, poderá haver imunidade total ou redução da penalidade aplicável de 1/3 a 2/3 também, não havendo, no âmbito civil, benefícios automáticos.

No entanto, a empresa e/ou pessoa física deve seguir alguns requisitos para a celebração do acordo, conforme os artigos 238 do Regimento Interno do Cade (RICade) e 86 da Lei nº 12.529/2011, tais como: *(i)* a empresa deve ser a primeira a se qualificar relativo à infração noticiada ou em investigação; *(ii)* a empresa e/ou pessoa física devem cessar a participação na infração noticiada ou em investigação; *(iii)* a Superintendência-Geral não dispor de provas suficientes que assegurem a condenação da empresa e/ou pessoa física; *(iv)* a empresa e/ou pessoa física deve confessar sua participação na prática ilícita; *(v)* a empresa e/ou pessoa física deve cooperar plenamente com a investigação e o processo administrativo; e *(vi)* deve resultar da cooperação a identificação dos demais envolvidos e dos documentos que comprovem a infração.

No que tange ao Termo de Compromisso de Cessação (TCC), disposto no artigo 85 da Lei nº 12.529/2011, pode ser celebrado entre o Cade e/ou pessoas físicas que estejam sendo investigadas por alguma infração à ordem econômica. Nesse acordo, o Cade concorda em suspender o prosseguimento das investigações em andamento relativas ao compromissário, desde que sejam cumpridos os termos do acordo. A possibilidade de celebração desse acordo se dá a fim de evitar gastos relacionados à litigância e à exposição da imagem da empresa por longos períodos. Soma-se a isso a mitigação da multa. No caso de cartéis, há sempre a exigência de recolhimento pecuniário devido à posição mais dura do Cade. Ainda, é importante destacar que quanto mais provas e o quanto antes essas provas forem produzidas, melhor será o acordo, sendo que o CADE sempre se baseia no limite do tamanho do benefício do último TCC firmado no mesmo caso[80].

Sendo assim, o TCC, de modo geral, possui as mesmas características do AL. Seus requisitos são: *(i)* pagar contribuição pecuniária ao Fundo de Defesa de Direitos Difusos – artigos 85, §1º, III, da Lei nº 12.529/2011 e 224 do RICade; *(ii)* o proponente deve reconhecer

[79] Idem.
[80] Deloitte. Orientações para celebração de acordos de cooperação por empresas. IBDEE, agosto de 2018. Pesquisa "Acordos de Cooperação – Percepção do Empresariado sobre o Tema e Práticas Adotadas", p. 16.

a participação na conduta investigada – artigo 225 do RICade; *(iii)* o proponente deve colaborar com a instrução processual – artigo 226 do RICade; *(iv)* o proponente não deve praticar a conduta investigada – artigo 85 da Lei nº 12.529/2011; e *(v)* pagar multa no caso de descumprimento das obrigações compromissadas.

Ademais, dentre seus benefícios, administrativamente há a redução da penalidade aplicável em faixas de desconto previstas. No entanto, no âmbito criminal e civil não há benefícios automáticos.

4.1.1.2 Leniência no Sistema Financeiro Nacional

O Acordo de Leniência no âmbito do Sistema Financeiro Nacional da Lei nº 13.506/2017 pode ser celebrado por pessoas físicas ou jurídicas, nos casos em que forem cometidas infrações graves e não graves, seja pelo Bacen ou pela CVM.

Devido à natureza jurídica do Banco Central do Brasil (Bacen) de autarquia federal vinculada ao Ministério da Fazenda e à sua missão de assegurar a estabilidade do poder de compra da moeda e um sistema financeiro sólido e eficiente, é possível realizar acordos de cooperação.

Já a Comissão de Valores Mobiliários (CVM) é uma entidade autárquica em regime especial que possui personalidade jurídica e patrimônio próprios. Apesar de ser vinculada ao Ministério da Fazenda, é dotada de autoridade administrativa independente, sem necessidade de se subordinar hierarquicamente, possuindo mandato fixo e estável de seus dirigentes. A ela é dada autonomia financeira e orçamentária. Devido ao seu propósito de zelar pelo funcionamento e integridade do mercado de capitais, dentre outros, foi concedida a possibilidade de celebrar termos de compromisso, fundamentada na Lei nº 6.385/76. O particular, ao celebrar o acordo, procura extinguir a punibilidade ou mitigar as penalidades cabíveis relativas à infração relatada, assim como nos termos de compromisso do Bacen[81].

Os requisitos desse acordo são os mesmos do Acordo de Leniência Antitruste, já citados. No entanto, seus benefícios divergem, sendo, no caso de leniência total, a imunidade total e, no caso de leniência parcial, a redução de 1/3 a 2/3 ou redução fixa de 1/3. Entretanto, tais benefícios administrativos não repercutem nos demais órgãos. Criminal e civilmente não há benefícios automáticos.

[81] Deloitte. Orientações para celebração de acordos de cooperação por empresas. IBDEE, agosto de 2018. Pesquisa "Acordos de Cooperação – Percepção do Empresariado sobre o Tema e Práticas Adotadas", p. 23.

O termo de compromisso, disposto na Lei no 13.506/2017 e na Circular no 3.857/2017, tem por objetivo dar eficiência à função de supervisão do BCB, garantindo seu caráter educativo. Assim, pode-se eliminar processos sancionatórios e proporcionar extinção de punibilidade ao particular em relação à infração relatada. Não podem ser celebrados acordos em caso de infrações graves, não podendo suspender o andamento do processo administrativo (art. 11, §§ 1º e 4º).

Assim como o termo de compromisso, o acordo de supervisão do BCB está disposto na na Lei no 13.506/2017 e na Circular nº 3.857/2017. Sua função, no âmbito do BCB, consiste em obter a cooperação do particular na identificação dos demais envolvidos na prática da infração relatada, se existentes, e na identificação de informações e documentos que comprovem a infração noticiada e/ou em investigação. Para o particular, a intenção é extinguir a punibilidade ou mitigar as penalidades cabíveis relativas à infração relatada[82].

Dentre os acordos que podem ser realizados com a CVM, há também o acordo de supervisão, instituído pelo artigo 34 da Lei nº 13.506/2017 que, por sua vez, dispõe que devem ser aplicadas as mesmas regras dos acordos de supervisão do Bacen, no que couber.

Diferentemente do acordo de leniência, o TCC possui como benefícios o pagamento de contribuição pecuniária para o Bacen e a não instauração ou suspensão de processos administrativos em face do compromissário.

4.1.1.3 Leniência Anticorrupção

O acordo de leniência da Lei nº 12.846/2013 pode ser celebrado desde 2013, após a edição da Lei Anticorrupção, por pessoas jurídicas que estejam envolvidas em prática de atos lesivos à administração pública nacional e/ou estrangeira. Anteriormente estava restrito às investigações relacionadas às práticas anticoncorrenciais. A possibilidade de celebração desse acordo e seus eventuais benefícios estão disciplinados nos artigos 16 e 17 da lei em questão, além da regulamentação federal através do Decreto nº 8.420/2015, que trata dos acordos de leniência em seus artigos 28 e 40.

O objetivo é que sejam alcançados resultados úteis decorrentes da cooperação da pessoa jurídica envolvida. Dessa forma, o Estado flexibiliza seu ônus de apurar a verdade dos fatos, transferindo-o à colaboradora[83]. Essa cooperação se dá pela prestação de informações e provas

[82] Deloitte. Orientações para celebração de acordos de cooperação por empresas. IBDEE, agosto de 2018. Pesquisa "Acordos de Cooperação – Percepção do Empresariado sobre o Tema e Práticas Adotadas", p. 21.
[83] Idem.

consistentes que possam ser agregadas à investigação. O artigo 16 da lei já citada prevê os requisitos necessários, tais como a identificação dos demais envolvidos na infração, se existir, e a obtenção veloz de informações e documentos que comprovem os atos ilícitos sendo investigados.

Como no acordo da Lei nº 12.529/2011, a pessoa jurídica deve seguir alguns outros requisitos para a celebração do acordo, tais como: *(i)* deve ser a primeira a se manifestar sobre seu interesse em cooperar com a apuração do ato ilícito; *(ii)* deve cessar a participação na infração noticiada a partir da data da propositura do acordo; e *(iii)* deve admitir sua participação no ilícito e cooperar plenamente com as investigações e o processo administrativo. Além disso, o acordo deve ser proposto pela pessoa jurídica interessada no máximo até a conclusão do relatório se já houver sido instaurado Processo Administrativo de Responsabilização, seja por via oral ou escrita.

Dentre seus benefícios, pode-se observar a isenção da obrigatoriedade de publicar a punição, a isenção da proibição de receber incentivos, subsídios e empréstimos públicos, a redução da multa em até 2/3 e a isenção ou atenuação da proibição de contratar com a Administração Pública[84]. No entanto, não existem benefícios criminais e civis automáticos.

4.1.1.4 Leniência do Ministério Público

Para as infrações previstas na Lei Anticorrupção e na Lei de Improbidade Administrativa, há a possibilidade da celebração do Acordo de Leniência do MP, previsto em diversos estatutos legais.

Devem-se observar alguns requisitos para a celebração de acordos com o MP, conforme a Orientação nº 07/2017 do MPF, tais como: *(i)* atender ao interesse público; *(ii)* apresentar informações e provas relevantes; *(iii)* cessar as práticas ilícitas; *(iv)* implementar programa de *compliance*; *(v)* colaborar plenamente com as investigações; e *(vi)* promover contribuições pecuniárias.

Dentre seus benefícios, há a definição das tratativas para a celebração do acordo, tendo como objeto os mesmos fatos em outras autoridades, a emissão de certidão sobre a extensão da cooperação realizada e retirada de eventuais restrições cadastrais[85]. No entanto, não há

[84] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 26.
[85] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 26.

benefícios administrativos automáticos. Criminalmente não haverá propositura de ações para os indivíduos de baixa culpabilidade, não havendo benefícios para os indivíduos de grave culpabilidade, que devem negociar a colaboração premiada. Também não serão propostas ações cíveis ou sancionatórias, devendo ser suspensas as já propostas ou haver prolação de decisão com efeitos meramente declaratórios[86].

Há, também, a possibilidade de celebração de acordos de colaboração premiada, destinado a pessoas físicas. Dentre seus benefícios, pode-se observar o perdão judicial, a redução em até 2/3 da pena privativa de liberdade ou substituição por pena restritiva de direitos. No entanto, não existem benefícios criminais e civis automáticos[87].

Diante do exposto, depreende-se que, para que seja possível cumprir com os requisitos para celebração dos acordos e gozar dos benefícios acordados, a empresa deve expor diversos dados pessoais dos envolvidos. Fato é que, até a LGPD, não havia preocupação com quais dados eram expostos, em que circunstâncias, como se dava o tratamento, armazenamento e exclusão desses dados. Agora, devem ser observados os requisitos dispostos para garantir a proteção dos dados pessoais.

Fato é que a procura por caminhos alternativos com menores punibilidades têm aumentado cada vez mais. Os benefícios que podem ser concedidos às empresas, pessoas físicas e jurídicas são atrativos e podem estimular a ultrapassagem de limites relativos aos direitos dos envolvidos, ou não, em práticas ilícitas. Nesse contexto, diante da variedade de acordos existentes, fez-se necessário mapear os limites de natureza, coleta, uso, armazenamento e exclusão de dados pessoais definidos na LGPD, conforme foi exposto no capítulo 3, devido ao alto número de pessoas que podem ser afetadas em investigações internas para verificação de tais práticas ilícitas após a celebração de acordos.

Depois de vistos os requisitos para celebração de acordos com a administração pública, com foco nos acordos de leniência e sem aprofundar os demais acordos, serão analisadas, a seguir, como se dá a observância das novas diretrizes da LGPD que devem ser aplicadas às investigações internas para que sejam celebrados acordos com a administração pública em concordância com a LGPD.

[86] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 26.
[87] ATHAYDE, Amanda. Manual dos Acordos de Leniência no Brasil: teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019. p. 26.

4.2 REQUISITOS DE OBSERVÂNCIA DA LGPD NA CELEBRAÇÃO DE ACORDOS DE COOPERAÇÃO COM A ADMINISTRAÇÃO PÚBLICA

Faz-se necessário, ainda, tratar das questões relacionadas à observância da LGPD quando da realização de investigações internas e os trâmites para celebração dos acordos com a administração pública. Diante da necessidade de geralmente enquadrar todo tratamento de dados em uma base legal determinada, faz-se necessário estudar as possibilidades previstas nos artigos 7º e 11 da LGPD, incluindo as hipóteses do consentimento e do legítimo interesse. É preciso compreender como se aplica cada base legal a fim de que seja garantida a segurança nas relações e evitado que os direitos e liberdades dos titulares sejam ameaçados ou sofram danos.

Para isso, serão analisadas com maior profundidade, inicialmente, as bases legais para o tratamento de dados pessoais na LGPD, principalmente o legítimo interesse (4.2.1), e a necessidade de consentimento dos titulares e seus tipos (4.2.2), para, em seguida, tratar dos diferentes tipos de funcionários das empresas que desencadeiam em diferentes quantidades de informações pessoais a serem coletadas (4.2.3).

4.2.1 O legítimo interesse do controlador de dados no uso das informações coletadas

Partindo da premissa de que todo dado pessoal possui valor é que a LGPD adotou o conceito amplo de dado pessoal. Isso se deve ao fato de ele ser relacionado a uma pessoa natural identificada ou identificável, mesmo que inicialmente não pareçam relevantes pois, se transferidos, cruzados ou organizados, podem acabar resultando em dados específicos de alguém, podendo conter, inclusive, dados sensíveis[88].

Dentre as hipóteses legais para tratamento de dados vistas no item 3.1.3, o legítimo interesse permite o tratamento de dados importantes que estejam vinculados ao escopo de atividades praticadas pelo controlador, desde que haja uma justificativa legítima. No entanto, as expectativas do titular dos dados possuem um papel relevante para sua aplicação, bem como devem ser considerados também os princípios da finalidade, da necessidade e da proporcionalidade da utilização desses dados.

[88] "Um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados insignificantes no contexto do processamento eletrônico de dados" (MARTINS, Leonardo (org.). Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244-245. Disponível em: http://www.kas.de/wf/doc/26200-1442-1-30.pdf. Acesso em: março de 2021.

No entanto, em um contexto de uma relação já preestabelecida entre o titular e o controlador, pode ser dispensável novo consentimento para outros usos desde que sejam implícitos. Ademais, quando o interesse for de terceiro, a base poderá ser aplicada em situações em que eles não tiverem meios para obter tal tipo de autorização ou se esse tipo de interação inviabilizar o próprio tratamento dos dados[89].

O interesse legítimo seria o controlador ou terceiro demonstrar ter algum benefício ou resultado claro e específico em mente, não bastando apenas que sejam interesses comerciais vagos ou genéricos, por exemplo. Ou seja, o objetivo precisa ser legítimo além de relevante. Alguns dos exemplos de prática do legítimo interesse, são:

> a) o tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controle de fraudes ou para garantir a segurança da rede e da informação nos sistemas informáticos de determinada instituição;
> b) fornecimento de imagens de câmeras de segurança para fins de seguro;
> c) segurança e melhoria de produtos e serviços;
> d) tratamentos de dados de empregados para programas de retenção de talentos e iniciativas de bem-estar;
> e) no caso de uso de dados por uma empresa para fazer ofertas mais adequadas e personalizadas a seus clientes, usando apenas os dados estritamente necessários para tal;
> f) envio de e-mail com descontos específicos para os produtos buscados por determinado usuário ou com indicações de compras, tomando como base seu histórico de compras;
> g) lembrar ao usuário que ele deixou itens no carrinho online, mas não finalizou a compra; e
> h) reunião de informações sobre determinado candidato em processos seletivos. Por ser um conceito em construção, caberá principalmente a Autoridade Nacional de Proteção de Dados (ANPD) e ao Poder Judiciário preenchê-lo no caso concreto[90].

Contudo, não há previsão de aplicação dessa hipótese legal na LGPD quanto aos dados sensíveis, que deve ser inserida nas bases legais dispostas no artigo 11.

Tendo em vista a necessidade de se dar maior concretude para a base legal do legítimo interesse, tanto a LGPD quanto o GDPR propõem alguns parâmetros interpretativos para sua aplicação. Sendo assim, deve-se realizar um teste de ponderação - o *legitimate interest assessment* (LIA)[91]. A finalidade desse teste é balancear os direitos do titular e do controlador,

---

[89] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 232.
[90] BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019.
[91] Grupo de trabalho do artigo 29º para a proteção de dados. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7º da Diretiva 95/46/CE. Adotado em 9 de abril de 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf. Acesso em março de 2021.

de modo a verificar se há um interesse legítimo do controlador como também se estão sendo respeitadas as legítimas expectativas, direitos e liberdades fundamentais dos titulares. Os artigos 7º, IX e 10 da LGPD, que tratam dos interesses legítimos, possibilitam a alteração de parte do mencionado teste para avaliar a existência de legítimo interesse no caso concreto.

Além disso, devem ser cumpridas quatro fases para se verificar o devido preenchimento do requisito do legítimo interesse, quais sejam: *(i)* a avaliação dos interesses legítimos; *(ii)* o impacto sobre o titular do dado; *(iii)* o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e *(iv)* as salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado[92].

A LGPD também estabelece parâmetros para a utilização do interesse legítimo como requisito autorizativo para o tratamento de dados sem o consentimento do titular, conforme o artigo 10:

> 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.

No caput e no inciso I acima, contém a necessidade de avaliação da existência de uma finalidade legítima e de uma situação concreta para o tratamento dos dados. Para Bioni[93], inicialmente, deve-se verificar se o interesse do controlador é legítimo, em outras palavras, se não contraria outros dispositivos legais. Nessa oportunidade, serão avaliados os benefícios ou vantagens que o controlador pode vir a ter, evitando o uso genérico dos dados. Além disso, é importante garantir que haja um caso concreto.

[92] PEREIRA DE SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais. Direito Público, v. 16, n. 90, dez. 2019.
[93] BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 237.

Enquanto o §1º traz o princípio da necessidade, devendo os dados pessoais ser realmente necessários para que a empresa alcance a finalidade pretendida. Já o inciso II traz a ideia do balanceamento de interesses entre as expectativas do titular, contendo seus direitos e liberdades, e o da empresa. Essa é a principal fase do teste de proporcionalidade, sendo que "Isso é parametrizado pela noção de compatibilidade entre o uso adicional e aquele que originou a coleta dos dados. Eles devem ser próximos um do outro, demandando-se uma análise contextual para verificar se esse uso secundário seria esperado pelo titular dos dados"[94]. Em se tratando de terceiro (pessoa sem relação preestabelecida com o titular), é muito mais difícil demonstrar o legítimo interesse, elevando o risco de utilização dessa base legal. Finalmente, os §§ 2º e 3º dispõem das salvaguardas como exigências de transparência e mecanismos de oposição.

Vale dizer, no entanto, que esse requisito apenas legitima o tratamento de dados pessoais definindo o limite necessário para a finalidade a qual ele se propõe, devendo o agente de tratamento realizar e manter o registro das operações de tratamento de dados que realizar, especialmente quando baseado no legítimo interesse, de acordo com o artigo 37. Justamente pela flexibilidade do legítimo interesse, recomenda-se que seja feito o relatório de impacto à proteção de dados pessoais, para que sejam minimizados os riscos para ambos os lados da relação.

Como o relatório poderá ser solicitado pela ANPD, deve-se documentá-lo, conforme o artigo 10º, § 3º da LGPD. Em outras palavras, deverá ter sido preparado quando da decisão de utilizar da base legal do legítimo interesse, antes de realizar o tratamento de quaisquer dados[95]. No entanto, o artigo 38 da mesma lei dispõe que o legislador, neste caso, não espera a prévia feitura do documento: "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".

Vale dizer que a devida utilização da base legal do legítimo interesse possibilita novos modelos de negócio e estratégias comerciais de segurança e inovação. Entretanto, deve-se equilibrar o legítimo interesse e as legítimas expectativas e direitos dos titulares. Conforme o artigo 7º, IX da LGPD, os interesses legítimos poderão ser do controlador ou de terceiros, podendo ser "interesses comerciais, individuais ou mesmo interesses da coletividade e da sociedade amplamente considerados"[96].

---

[94] Ibidem.
[95] LEONARDI, Marcel. Legítimo interesse. Revista do Advogado, v. 39, 2019, p. 70.
[96] Ibidem.

Contudo, o artigo 10 da LGPD faz referência apenas ao controlador, de modo que a doutrina e a ANPD devem esclarecer se sua interpretação deverá ser ampliada ou não. O termo "terceiro" não se refere apenas a outras organizações, também pode ser um indivíduo que não estivesse envolvido inicialmente de forma direta na relação ou o público em geral.

Diante do exposto, conclui-se que o legítimo interesse: *(i)* pode ser a base legal mais apropriada em diversas hipóteses, devendo, no entanto, ser aplicada de forma proporcional e limitada, quando trouxer benefício claro e determinado para o controlador e/ou terceiro; *(ii)* poderá ser aplicado quando não causar alto impacto aos direitos e garantias do indivíduo; *(iii)* o indivíduo titular dos dados deverá esperar que seus dados sejam usados razoavelmente; e *(iv)* poderá ser aplicado quando não for possível ou não se desejar dar ao titular dos dados total controle ou quando o controlador não quiser incomodá-lo com solicitações de consentimento para tratamentos que muito provavelmente seriam aceitos pelo titular.

Após analisada a base legal do legítimo interesse, será analisada a necessidade de consentimento dos titulares e seus tipos, conforme será feito a seguir.

4.2.2 O consentimento dos titulares dos dados como principal requisito

Um dos requisitos mais importantes que deve ser observado para cumprimento da LGPD é o devido consentimento dos titulares dos dados. Sendo assim, para que sejam respeitadas as diretrizes da LGPD quando da celebração de acordos de cooperação, deve haver o prévio consentimento dos funcionários para que seus dados sejam tratados e utilizados para tal finalidade.

Vale dizer que, no Brasil, convencionou-se que apenas os portadores de CPF são titulares de dados, conforme a LGPD, ao passo que portadores de CNPJ não. Contudo, se houver fato explícito que comprove a má conduta do funcionário, poderá ser desnecessário o consentimento do titular para uso dos dados, devendo ser respeitados os limites para garantir a proteção de dados do funcionário.

Conforme já exposto, a LGPD traz onze hipóteses autorizativas para o tratamento de dados pessoais, dentre elas, o fornecimento de consentimento pelo titular, previsto no art. 7º, I, da LGPD. Sendo assim, é necessário abordar como se dá esse consentimento, que deve ser uma manifestação do titular livre, informada e inequívoca.

Consentimento é a concordância de vontades em uma relação jurídica, ou seja, um consenso mútuo, por meio de uma uniformidade de opinião. Especificamente, o consentimento

do titular dos dados pessoais é um dos pontos fundamentais da LGPD. Para o direito contratual, consentimento é tido como "aceitação é o ato pelo qual uma pessoa manifesta, de modo inequívoco, seu consentimento às cláusulas de um contrato. Por meio da aceitação, aperfeiçoa-se o vínculo contratual"[97]. Já para Mendes e Doneda:

> Os requisitos para que um consentimento seja considerado válido pela lei estão previstos já na sua definição (artigo 5º, XII), segundo o qual o consentimento deve ser livre, informado, inequívoco e com uma finalidade determinada. Em caso de tratamento de dados sensíveis, o consentimento deve ser ainda fornecido ainda de forma específica e destacada, nos termos do artigo 11, I, da LGPD. Caso o consentimento seja formulado de forma genérica ou a partir de informações enganosas prestadas ao titular, o consentimento será nulo, conforme determinam respectivamente os artigos 8º, §§ 4º e 9º, § 1º da lei[98].

Em seu artigo 5º, XII, a LGPD define o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". No entanto, de acordo com o artigo 8º da LPGD confere que o consentimento deve ser fornecido por escrito ou por outra forma que assegure a manifestação de vontade por parte do titular. Esse artigo também trata das regras relativas à forma e finalidades do fornecimento do consentimento, tais como:

> § 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.

[97] SILVA, De Plácido e. Vocabulário jurídico. 28. ed. Rio de Janeiro: Forense, 2009. p. 48.
[98] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, Brasília, v. 120/2018, p. 471, nov./dez. 2018.

O § 1º do art. 9º, que trata dos direitos dos titulares dos dados, elucida sobre a nulidade do consentimento nos casos em que o titular tenha sido exposto a conteúdo enganoso ou abusivo, ou que não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca[99]. Já o § 2º explica que, se o consentimento foi requerido, mas houve mudanças da finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre tais mudanças, podendo o titular revogar o consentimento se discordar das alterações. Por fim, o § 3º do artigo em questão trata das situações em que 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 (artigo 18).

A LGPD também prevê que o ato de consentir deve ser praticado pela pessoa natural titular dos dados, ou por seu responsável legal, de forma evidente e inequívoca, por escrito ou não. Além disso, nos casos de tratamento de dados sensíveis ou de dados de crianças e adolescentes o consentimento possui características adicionais, como por exemplo, o manifestado consentimento de forma específica e destacada, com a obrigatoriedade do assentimento de pelo menos um dos pais ou do responsável legal.

Em síntese, o consentimento na LGPD, para não configurar vício de vontade e ser considerado nulo, deve ser: *(i)* livre; *(ii)* informado; *(iii)* inequívoco; e *(iv)* com finalidade determinada. Para ser livre, o titular deve ter controle sobre o tratamento de seus dados pessoais, podendo escolher quais dados quer fornecer e retirar seu consentimento a qualquer momento. No entanto, deve-se apartar o consentimento de dados essenciais dos não essenciais, ficando a cargo do titular autorizar o uso de dados pessoais não obrigatórios para determinado fim, caso em que apenas os dados necessários para a prestação de serviços podem ser considerados obrigatórios.

O consentimento informado, por sua vez, consiste em garantir que o titular tenha informações suficientes sobre a empresa que fará o tratamento dos seus dados pessoais para que possa decidir conscientemente[100]. Para isso, devem ser informadas, no mínimo a identidade da empresa responsável pelo tratamento e as finalidades deste. No caso de erro, dolo ou coação, há vício de consentimento resultante na nulidade da aceitação do titular.

---

[99] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. Revista de Direito do Consumidor, Brasília, v. 120/2018, p. 471, nov./dez. 2018.

[100] SILVA, De Plácido e. Vocabulário jurídico. 28. ed. Rio de Janeiro: Forense, 2009.

Já o consentimento inequívoco sujeita-se a uma manifestação por meio de um ato positivo do titular, não bastando a aceitação passiva, ou seja, o silêncio não pode ser considerado como consentimento. Por fim, o consentimento deve ter finalidade específica e determinada, ao passo que o tratamento deve sempre estar vinculado a uma ou mais finalidades específicas que devem ser informadas ao titular. É obrigatório o uso de dados pessoais para fins não conhecidos pelo titular, cabendo ao controlador ou operador informar a forma, a duração e a finalidade do tratamento dos dados, conforme será visto no próximo capítulo.

Depreende-se, assim, que o instituto do consentimento possibilita ao titular condições de escolher produtos ou serviços que coletem seus dados pessoais, podendo dar consentimento específico para determinado tipo de tratamento e não para os outros pretendidos pelo controlador ou operador. Além disso, o titular pode revogar o seu consentimento a qualquer tempo.

No entanto, no caso dos funcionários de empresas que venham a celebrar acordos de cooperação, há que de destacar que os dados de diferentes funcionários são exigidos e monitorados em diferentes graus, dependendo de seu cargo, como conselheiros, diretores e demais funcionários. Nesse caso, os dados pessoais necessários, obrigatórios ou não, devem ser distintos. Percebe-se, então, a necessidade de verificar essa discrepância, conforme será feito a seguir.

4.2.3 Proposta de condições particulares de diferentes hierarquias de funcionários

Como o instituto do consentimento possibilita ao titular de dados condições de escolher produtos ou serviços que coletem seus dados pessoais, no caso das empresas, os funcionários podem fazê-lo. Há, no entanto, uma diferença entre os dados que são coletados de funcionários que não exercem cargos diretivos na entidade dos que exercem, como diretores e conselheiros. Sendo assim, devem ter requisitos diferentes para colher dados dos diferentes funcionários da organização.

No caso dos funcionários de empresas que venham a celebrar acordos de cooperação, há que de destacar que os dados de diferentes funcionários são exigidos em diferentes graus, dependendo de seu cargo, como conselheiros, diretores e demais funcionários. Nesse caso, os dados pessoais necessários, obrigatórios ou não, devem ser distintos. Percebe-se, então, a necessidade de identificar os dados pessoais que devem ser coletados conforme os diferentes cargos das empresas, apesar de não haver normatização sobre o tema.

Para os funcionários que não exercem cargos diretivos, são coletados os dados pessoais considerados comuns para realização de cadastros e compor a relação contratual, como nome completo, endereço, comprovante de residência, CPF, telefone, nome dos pais, endereço eletrônico, informações dos filhos e dependentes. Percebe-se que, já no caso dos funcionários apesar de não serem necessárias grandes quantidades de informações pessoais, são necessários dados sensíveis, muitas vezes, de menores de idade, que são seus filhos e dependentes. Esses dados devem ser tratados, armazenados e excluídos com muito mais cuidado, conforme visto no capítulo 3.

Já dos funcionários que exercem atividades diretivas, como diretores e conselheiros, são solicitadas informações adicionais não comuns em simples relações de emprego, como os dados para preenchimento da relação de partes relacionadas. Apesar da não obrigatoriedade de todos os tipos de empresas de instituírem políticas que regulem as relações com as partes relacionados de dirigentes, a maioria a implanta, apesar da escassa doutrina a respeito da matéria.

Isso acontece para que estejam em conformidade com os requisitos de competitividade, conformidade, transparência, equidade e comutatividade. Dessa forma, é uma boa prática que deve ser observada pela governança corporativa da entidade. Para isso, são solicitadas diversas informações sobre o funcionário e todos os seus familiares, filhos, pais, irmãos, etc. Para melhor compreensão, partes relacionadas são as pessoas ou entidades que estão relacionadas com a entidade que está elaborando suas demonstrações contábeis, como uma pessoa, ou um membro próximo da família, que está relacionada com a entidade que reporta a informação: *(i)* se tiver o controle pleno ou compartilhado da entidade que reporta a informação; *(ii)* se tiver influência significativa sobre a entidade que reporta a informação; e *(iii)* se for membro do pessoal chave da administração da entidade que reporta a informação ou da controladora da entidade que reporta a informação.

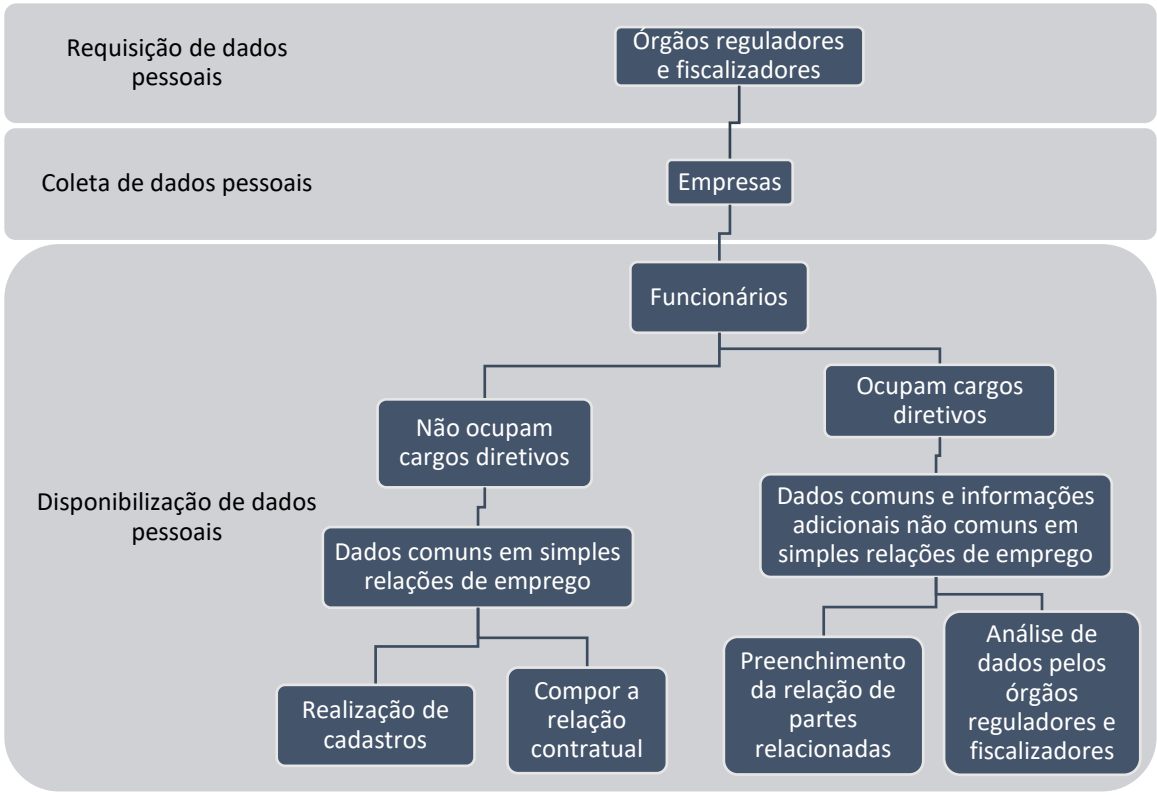
Em complemento, há também os casos de entidade que está relacionada com a entidade que reporta a informação se qualquer das condições seguintes for observada: *(i)* a entidade e a entidade que reporta a informação são membros do mesmo grupo econômico - quando a empresa controladora e cada controlada são inter-relacionadas, bem como as entidades sob controle comum são relacionadas entre si; *(ii)* a entidade é coligada ou controlada em conjunto (*joint venture*) de outra entidade - ou coligada ou controlada em conjunto de entidade membro de grupo econômico do qual a outra entidade é membro; *(iii)* ambas as entidades estão sob o controle conjunto (*joint ventures*) de uma terceira entidade; *(iv)* uma entidade está sob o controle conjunto (*joint venture*) de uma terceira entidade e a outra entidade for coligada dessa

terceira entidade; *(v)* a entidade é um plano de benefício pós-emprego cujos beneficiários são os empregados de ambas as entidades, a que reporta a informação e a que está relacionada com a que reporta a informação (se a entidade que reporta a informação for ela própria um plano de benefício pós-emprego, os empregados que contribuem com a mesma serão também considerados partes relacionadas com a entidade que reporta a informação); *(vi)* a entidade é controlada, de modo pleno ou sob controle conjunto, por uma pessoa identificada; e *(vii)* uma pessoa identificada tem influência significativa sobre a entidade, ou for membro do pessoal chave da administração da entidade (ou de controladora da entidade).

Há, também, os casos de entidades reguladas pelo Bacen e pela CVM, que devem consolidar praticamente um dossiê sobre os diretores e conselheiros eleitos e encaminhar para que os órgãos em questão analisem as informações pessoais de cada um, a fim de que aprovem a posse de tais cargos ou não. Isso ocorre para que os diretores e conselheiros cumpram com os requisitos de ocupação de cargos do tipo e sejam avaliados os possíveis riscos para a instituição.

Diante desses diferentes tipos de funcionários e os diferentes dados solicitados para cada um, é preciso que a organização se adapte, principalmente o RH. Uma das primeiras ações que devem ser realizadas é identificar quais são as informações dos colaboradores que estão sob responsabilidade da área e de que forma estão armazenadas, além de por quanto tempo é preciso guardar esses dados e como protegê-los durante a permanência do colaborador na empresa, para que outros colaboradores não tenham acesso.

Para melhor entendimento, o fluxo descrito está exemplificado abaixo:



Elaborado pela autora.

Sendo assim, cada empresa deve se realizar questionamentos para atender às suas necessidades próprias, visto que dificilmente encontrarão fórmulas prontas, tais como: *(i)* quais são os dados que devem ser legalmente mantidos para atendimento do eSocial e outras requisições trabalhistas; *(ii)* quais dados requerem o consentimento do candidato e colaboradores; *(iii)* quais são os dados imprescindíveis ao desenvolvimento da atividade laboral como formação, registro profissional, certidões negativas etc.; *(iv)* por quanto tempo será necessário manter esses dados armazenados; *(v)* como é possível proteger os dados armazenados dos candidatos e colaboradores; *(vi)* quais são os dados disponíveis e que podem ser descartados; *(vii)* quais são os dados que devem ser mantidos e dependem de autorização do colaborador titular para armazenamento e tratamento; entre outros.

Os maiores impactos se dão nos processos de recrutamento e seleção, pois será importante que os responsáveis pela TI e RH reestruturem as políticas e os acordos de confidencialidade.

Percebe-se, diante do exposto, que os dados dos funcionários são colhidos em graus distintos a depender do cargo que exercem. Assim, há um maior nível de exposição por parte dos funcionários que exercem funções diretivas nas entidades e, apesar de não haver legislação que regule a tipo das informações que podem ser solicitadas, a fim de que tais funcionários

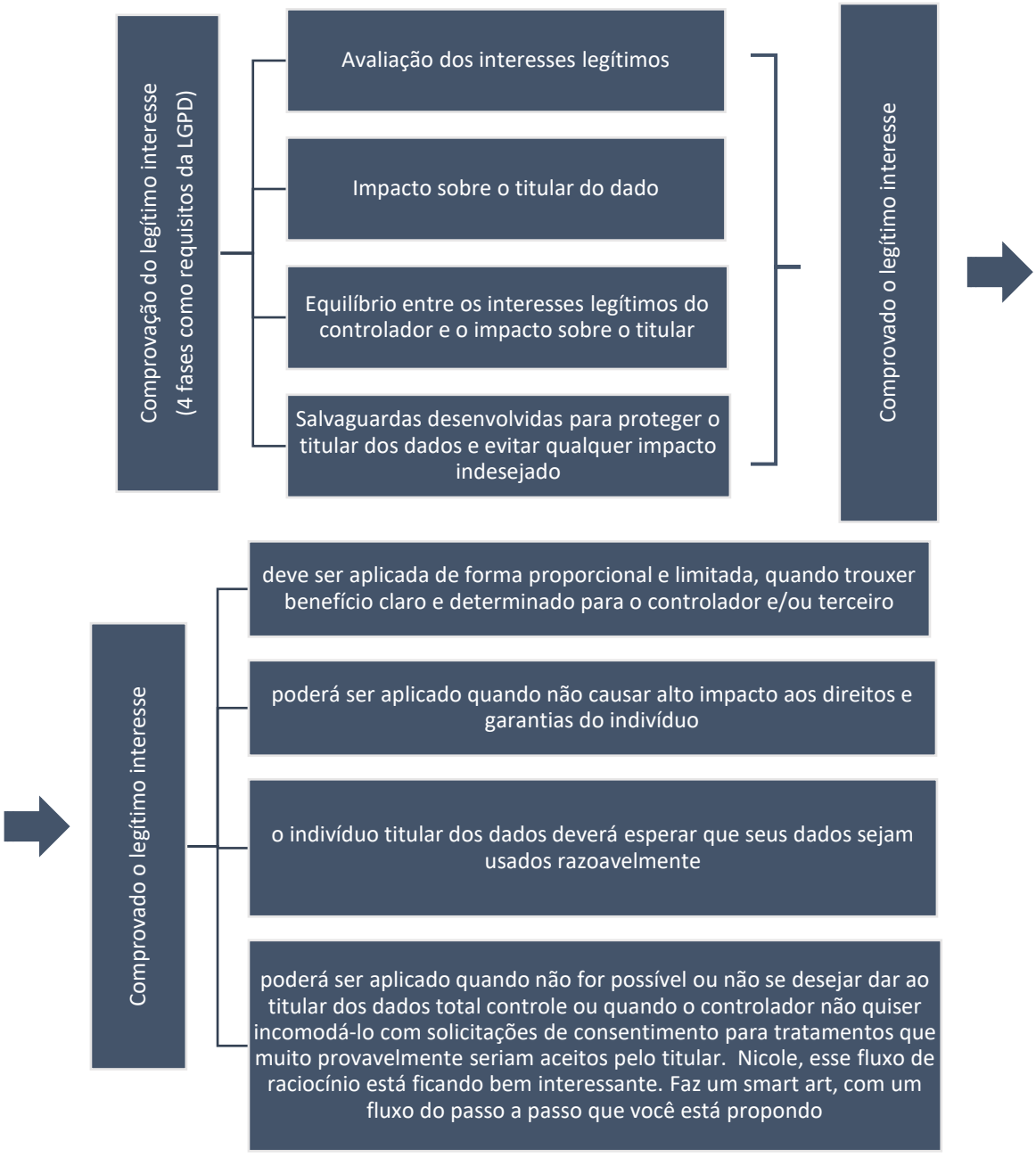
sejam resguardados e não tenham que fornecer informações pessoais desnecessárias, as empresas devem realizar uma análise interna e elencar quais informações são necessárias para atender às solicitações dos órgãos reguladores e, eventualmente, questioná-los sobre a real necessidade daquela informação.

Após tratar do consentimento dos titulares e seus tipos como principal requisito para o tratamento de dados pessoais, foram expostos os diferentes tipos de funcionários das empresas que desencadeiam em diferentes quantidades de informações pessoais a serem coletadas.

Aqui, vale lembrar algumas perguntas realizadas no capítulo 1: *(i)* quais são os requisitos definidos pela LGPD para que a empresa possa utilizar dados de trabalhadores obtidos em investigações internas de *compliance* para a celebração de acordos com a administração pública quando tal trabalhador não é colaborador do acordo; e *(ii)* se os dados pessoais coletados pelas empresas, seja rotineiramente ou por meio de investigações internas realizadas por seus programas de *compliance*, podem ser utilizados para atender ao interesse dela quando da celebração de acordos com a administração pública.

Diante do exposto até aqui, inicialmente, como requisitos da LGPD, conclui-se que devem ser cumpridas quatro fases para se verificar o devido preenchimento do requisito do legítimo interesse, quais sejam: *(i)* a avaliação dos interesses legítimos; *(ii)* o impacto sobre o titular do dado; *(iii)* o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e *(iv)* as salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado.

Preenchidos os requisitos do legítimo interesse, percebe-se que ele: *(i)* pode ser a base legal mais apropriada em diversas hipóteses, devendo, no entanto, ser aplicada de forma proporcional e limitada, quando trouxer benefício claro e determinado para o controlador e/ou terceiro; *(ii)* poderá ser aplicado quando não causar alto impacto aos direitos e garantias do indivíduo; *(iii)* o indivíduo titular dos dados deverá esperar que seus dados sejam usados razoavelmente; e *(iv)* poderá ser aplicado quando não for possível ou não se desejar dar ao titular dos dados total controle ou quando o controlador não quiser incomodá-lo com solicitações de consentimento para tratamentos que muito provavelmente seriam aceitos pelo titular. Para melhor entendimento, o fluxo descrito está exemplificado abaixo:



Elaborado pela autora.

Depreende-se, portanto, que os dados pessoais coletados pelas empresas, seja rotineiramente ou por meio de investigações internas realizadas por seus programas de *compliance*, podem ser utilizados para atender ao interesse dela quando da celebração de acordos com a administração pública, desde que cumpridos os requisitos apresentados.

Em continuidade ao estudo, será abordado, no próximo capítulo, a relação entre os dados pessoais, o *compliance* e as investigações internas, contendo, na primeira parte, análises sobre as etapas da proteção de dados pessoais, a responsabilidade civil prevista na LGPD e as sanções

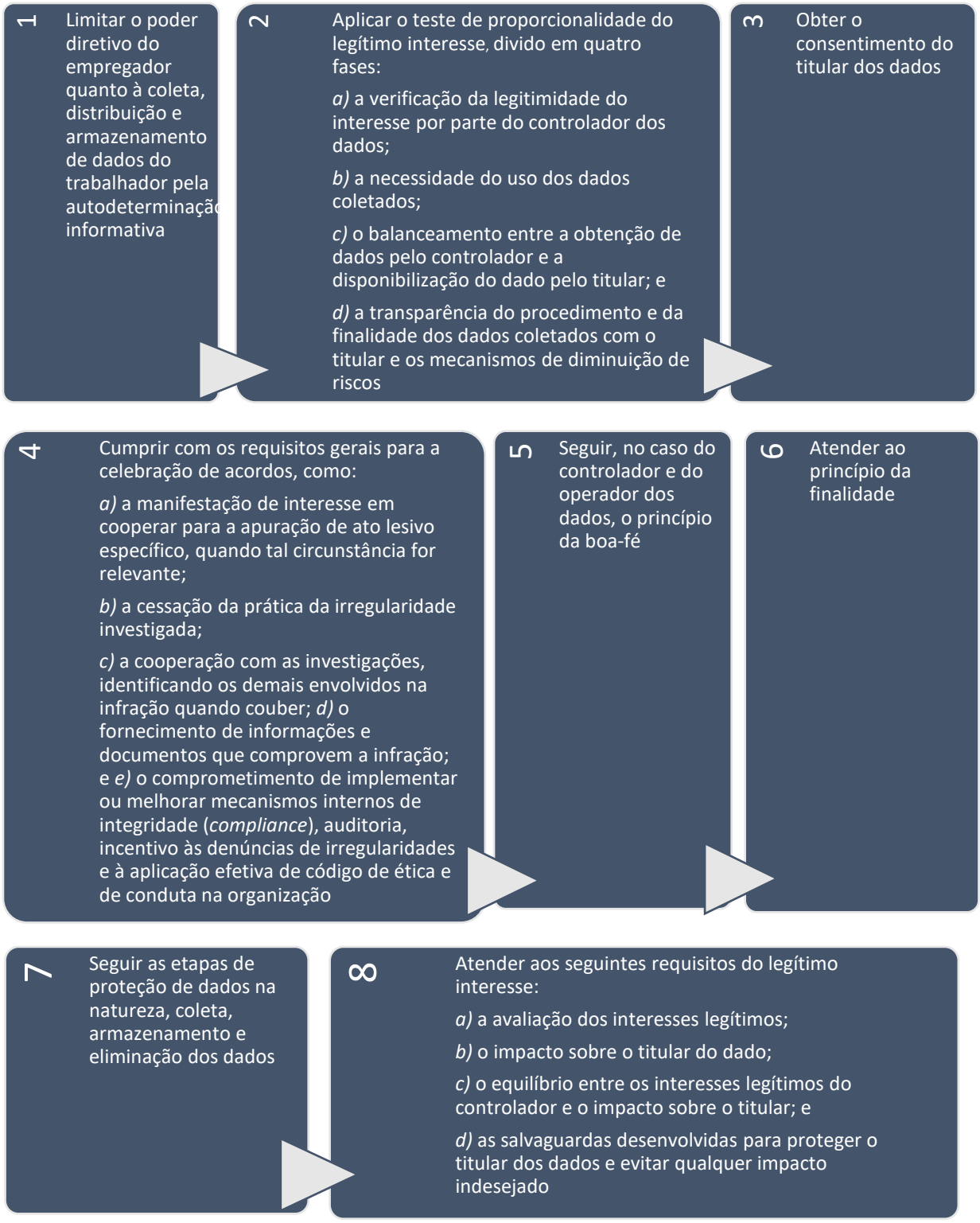
previstas de aplicação pela ANPD. Na segunda parte, serão abordados o *compliance*, diferenciando-o da governança corporativa, e as investigações internas.

4.2.4 Síntese dos requisitos para celebração de acordos de cooperação com a Administração Pública em conformidade com a LGPD

Analisadas as hipóteses do consentimento e do legítimo interesse, é preciso sintetizar todos os requisitos elencados ao longo do trabalho para a celebração de acordos de cooperação com a Administração Pública de modo a estar em conformidade com a LGPD.

Para isso, devem ser observados os seguintes requisitos dispostos a seguir para garantir a proteção dos dados pessoais: *(i)* limitar o poder diretivo do empregador quanto à coleta, distribuição e armazenamento de dados do trabalhador pela autodeterminação informativa; *(ii)* aplicar o teste de proporcionalidade do legítimo interesse, divido em quatro fases: *a)* a verificação da legitimidade do interesse por parte do controlador dos dados; *b)* a necessidade do uso dos dados coletados; *c)* o balanceamento entre a obtenção de dados pelo controlador e a disponibilização do dado pelo titular; e *d)* a transparência do procedimento e da finalidade dos dados coletados com o titular e os mecanismos de diminuição de riscos; *(iii)* obter o consentimento do titular dos dados; *(iv)* cumprir com os requisitos gerais para a celebração de acordos, como: *a)* a manifestação de interesse em cooperar para a apuração de ato lesivo específico, quando tal circunstância for relevante; *b)* a cessação da prática da irregularidade investigada; *c)* a cooperação com as investigações, identificando os demais envolvidos na infração quando couber; *d)* o fornecimento de informações e documentos que comprovem a infração; e *e)* o comprometimento de implementar ou melhorar mecanismos internos de integridade (*compliance*), auditoria, incentivo às denúncias de irregularidades e à aplicação efetiva de código de ética e de conduta na organização; *(v)* seguir, no caso do controlador e do operador dos dados, o princípio da boa-fé; *(vi)* atender ao princípio da finalidade; *(vii)* seguir as etapas de proteção de dados na natureza, coleta, armazenamento e eliminação dos dados; e *(viii)* atender aos seguintes requisitos do legítimo interesse: *a)* a avaliação dos interesses legítimos; *b)* o impacto sobre o titular do dado; *c)* o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e *d)* as salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado.

Para melhor entendimento, observe o esquema abaixo:



Elaborado pela autora.

4.3 A CORRELAÇÃO DAS INVESTIGAÇÕES INTERNAS DOS PROGRAMAS DE *COMPLIANCE* COM A LGPD: ATUAÇÃO E RESPONSABILIDADES

As empresas estão expostas a diversos riscos relativos a fraudes e corrupção. Igualmente, estão sujeitas a riscos decorrentes da conduta antiética dos funcionários. Buscando resolver seus problemas e mitigar esses riscos, cada vez mais as investigações internas de *compliance* estão ganhando força no meio corporativo.

Para isso, é necessário que seja realizada uma investigação interna independente e analítica para prevenir e detectar atividades e/ou processos em desacordo com as políticas internas, os regulamentos e as leis. Essa é a principal forma de proteger os interesses dos acionistas da companhia e da organização.

Fato é que as etapas de proteção de dados vistas no capítulo 3 entrosam com os programas de *compliance* da governança corporativa e com as investigações internas, conforme será exposto na segunda parte desse capítulo, bem como a responsabilidade civil decorrente dessa relação.

Dito isso, trataremos nos subitens abaixo, em um primeiro momento, da governança corporativa, essencial para tratar sobre o *compliance* e as investigações internas realizadas por este programa. Em seguida, serão abordadas as investigações internas e suas relações com a LGPD e os programas de *compliance*, inclusive sua responsabilidade na implantação da LGPD nas empresas, abordando sua atuação e responsabilidades previstas para esses casos. Para isso, será abordada a diferença entre governança corporativa e os programas de *compliance*, bem como os requisitos para sua eficácia.

4.3.1 Governança Corporativa e Compliance: diferenças e semelhanças

De início, é necessário conceituar governança corporativa, depois, explicar sua relação com os programas de *compliance* e as investigações internas. Sendo assim, governança corporativa é, para o Instituto Brasileiro de Governança Corporativa (IBGC)[101], "o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas".

Por isso, é de bom tom que os operadores e demais responsáveis formulem regras de boas práticas e de governança a fim de estabelecer as condições de organização, funcionamento, procedimentos, normas de segurança, padrões técnicos, ações educativas, obrigações

[101] IBGC. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa#:~:text=Governan%C3%A7a%20corporativa%20%C3%A9%20o%20sistema,controle%20e%20demais%20partes%20interessadas. Acesso em: janeiro de 2021.

específicas para os agentes de tratamento, mecanismos de supervisão e mitigação de riscos, entre outros. Com uma estratégia ampla, a governança corporativa busca, principalmente, garantir a confiança dos stakeholders. Para isso, se utiliza de 4 fundamentos: transparência, equidade, prestação de contas e responsabilidade corporativa.

Sobre o tratamento de dados, é importante levar em consideração a natureza, o escopo, a finalidade e a probabilidade e gravidade dos riscos e benefícios relacionados. O responsável por esse trabalho poderá realizar algumas ações, como: *(i)* implementar programa de governança em privacidade que: a) demonstre o comprometimento do responsável 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 em que 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 à 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 do órgão competente ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta; *(iii)* publicar e atualizar as regras de boas práticas e de governança periodicamente, podendo ser reconhecidas e divulgadas pelo órgão competente; e *(iv)* estimular, por meio do órgão competente, a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

Já o programa de *compliance* é uma estratégia mais específica que, em vez de focar na cultura geral da empresa e na relação com os stakeholders, busca manter a empresa de acordo com normas e leis. Na verdade, é um conjunto de esforços e estratégias que uma organização utiliza para que seus membros cumpram as normas legais e regulamentares, incluindo políticas e diretrizes procedimentais e éticas[102]. Essas ações objetivam, com o cumprimento dos preceitos

[102] ARTESE, Gustavo. Compliance digital: proteção de dados pessoais. In: CARVALHO, André Castro et. al. Manual de Compliance. Rio de Janeiro: Forense, 2019. p. 477.

normativos, prevenir a prática de atos ilícitos, minorar seus efeitos ou, ainda, sancionar os responsáveis[103]. Nesse sentido, Frazão[104], refere-se à *compliance* como:

> Ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade.

Dessa forma, os programas de *compliance* são ferramentas de Governança Corporativa "tendentes a garantir que as políticas públicas sejam implantadas com maior eficiência"[105]. E é por isso que ele apresenta um sentindo abrangente, não apenas do simples cumprimento de normas jurídicas e condutas éticas, mas também como um modo de mitigar riscos e garantir a sustentabilidade corporativa[106]. Dessa forma, viabiliza eventual descumprimento e os danos causados, para que sejam reduzidos os prejuízos, bem como seja criada uma cultura corporativa em conformidade com as normas jurídicas, que podem vir a atenuar sanções administrativas[107].

Com origem do verbo inglês *to comply*, a expressão *compliance* significa conformidade, ou seja, agir segundo a lei – vale também para instrução interna e preceitos éticos[108]. Possui 9 pilares, quais sejam: *(i)* dar suporte à alta administração; *(ii)* avaliar riscos; *(iii)* instituir e fazer cumprir o Código de conduta e as políticas de *compliance*; *(iv)* realizar a prática de controles internos; *(v)* realizar treinamentos e comunicações; *(vi)* disponibilizar e acompanhar os canais de denúncia; *(vii)* realizar investigações internas; *(viii)* realizar *due diligence*; e *(ix)* realizar auditoria e monitoramento.

É através dos controles internos, dos treinamentos, das auditorias e do apoio da alta administração que a empresa consegue provar que está em conformidade com todas as leis relacionadas a ela. De acordo com o ramo de atuação da empresa, podem existir programas de *compliance* mais específicos, como *compliance* ambiental, anticorrupção, de dados etc. No

---

[103] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 683.
[104] Ibidem.
[105] CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 53.
[106] BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de Compliance. Rio de Janeiro: Forense, 2019. p. 35.
[107] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 686.
[108] BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et. al. Manual de Compliance. Rio de Janeiro: Forense, 2019. p. 35.

entanto, é possível focar em processos e leis mais gerais, como a Lei Anticorrupção, aplicável à todas as empresas.

Há, essencialmente, uma diferença entre Governança Corporativa e *compliance*. A primeira possui o objetivo de demonstrar confiança e responsabilidade aos stakeholders, enquanto a segunda é uma forma utilizada para isso[109]. Ou seja, o programa de *compliance* é uma parte da estratégia maior da governança.

Vale citar, também, o programa de integridade, muito confundido com o programa de *compliance*. A diferença consiste no objetivo, já que *compliance* foca em estar de acordo com leis e normas, e a integridade foca na prevenção a atos ilícitos e antiéticos cometidos por funcionários ou terceiros. Em outras palavras, o programa de integridade foca nos representantes da empresa, buscando criar uma cultura ética e de integridade para que sejam minimizados riscos decorrentes de corrupção ou falta de *compliance*. São 5 os pilares do programa de integridade, que é uma das formas de atingir o objetivo do *compliance*: *(i)* comprometimento e apoio da alta direção; *(ii)* definição de instância responsável; *(iii)* análise de perfil e riscos; *(iv)* estruturação das regras e instrumentos; e *(v)* estratégias de monitoramento contínuo. Ademais, soma-se isso à criação de normas e políticas corporativas, como códigos de ética ou conduta.

Conclui-se, portanto, que a governança corporativa é uma estratégia ampla que engloba o programa de *compliance* – estratégia mais específica que a permite atingir seus objetivos, enquanto, por sua vez, o programa de *compliance* engloba o programa de integridade - estratégia mais específica ainda que o permite atingir seus objetivos, também. Conforme visto, devido a importância do *compliance*, é necessário avaliar os requisitos necessários para garantir a eficácia destes programas, assunto que será tratado no subitem a seguir.

4.3.1.1 Requisitos para a eficácia dos programas de compliance

No contexto apresentado, faz-se necessário atender a alguns requisitos para que seja assegurada a efetividade dos programas de *compliance*, como, por exemplo: *(i)* análise de riscos; *(ii)* código de ética; *(iii)* suporte da alta administração; *(iv)* treinamentos periódicos; *(v)* cultura corporativa; *(vi)* acompanhamento dos controles e processos internos; *(vii)* canais de comunicação; e *(viii)* apuração e punição de condutas contrárias ao programa.

[109] CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 53.

Para Frazão, Oliva e Abilio[110], deve ser realizada, inicialmente, a análise de riscos para que sejam identificados pontos vulneráveis na organização, evitando que não sejam cumpridas normas e de forma a providenciar medias preventivas para as vulnerabilidades identificadas. Essa análise e o seu acompanhamento são de extrema importância, devendo ser atualizadas conforme as normas. Dessa forma, podem ser criadas ferramentas de controle interno para inibir a prática de atos ilícitos[111].

Depois de identificados os riscos, deve-se tomar medidas para mitigá-los. Assim, é necessário elaborar Códigos de Ética e de Conduta, para que sejam consolidados princípios e valores da entidade, esclarecidas as condutas permitidas, ou não, e os canais de orientação e dúvidas[112]. O código se aplica a funcionários e a terceiros, devendo ser um documento da fácil acesso e leitura. Além disso, é essencial que haja suporte da alta administração por meio da disseminação da cultura corporativa e da participação ativa em eventos, treinamentos e supervisionando o programa, pois "[...] caso a gerência da pessoa jurídica manifeste-se de forma contraditória com os planos constantes no programa de *compliance*, a mensagem recebida pelos funcionários será de que esse não passa de simples instrumento de fachada"[113].

No entanto, devem ser garantidas a autonomia e a independência aos responsáveis por instituir os procedimentos e controles internos, supervisionar o programa de *compliance* e tomar as decisões que se façam necessárias. Ademais, são os treinamentos que possibilitarão que toda organização compreenda as normas aplicáveis a cada área. É necessário, também, que seja realizado o acompanhamento do cumprimento dos propósitos previstos no programa de *compliance*, sendo necessário evidenciar esse trabalho. Isso permitirá perceber se há correção e reação adequadas às falhas e violações da cultura da lei. Os parceiros comerciais e os mecanismos de controle por eles adotados devem ser analisados também.

Frazão, Oliva e Abilio expressam bem os resultados dessa ação no seguinte trecho: "o emprego do resultado dessa vigilância na constante atualização e aprimoramento do programa de *compliance* indica o compromisso da pessoa jurídica com o cumprimento da lei – quanto mais célere a mudança, maior o comprometimento"[114].

---

[110] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 687.
[111] Ibidem. p. 687.
[112] Ibidem. p. 689.
[113] Ibidem. p. 690.
[114] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 690.

Já os canais de comunicação são importantes para que os funcionários possam esclarecer e sanar dúvidas em relação a comportamentos e realizar denúncias, devendo ser mantido o sigilo para que o funcionário não sofra retaliações e não deixe de recorrer a esse meio. Há alguns pontos positivos nessa ação: *(i)* auxilia na prevenção da ocorrência de atos ilícitos; *(ii)* difunde comportamentos de conformidade; *(iii)* colabora para que as empresas fiquem cientes de ilicitudes cometidas; e *(iv)* colabora para que as empresas adotem medidas para impedir e prevenir novas condutas ilícitas.

Por fim, vale ressaltar que toda e qualquer denúncia recebida deve ser apurada e, se necessário, aplicadas sanções disciplinares. É por meio de tratamento igualitário para todos que será garantida a credibilidade da organização, bem como o comprometimento de que serão tomadas medidas céleres para que sejam adequados os procedimentos às normas, além das penalidades[115].

Conforme exposto, dentro dos programas de *compliance* podem existir subáreas específicas, como o *compliance* de dados pessoais, muito relevante no contexto dessa pesquisa. Por isso, será abordado, em seguida, a repercussão da adoção de programas desse tipo pelas empresas.

4.3.1.2 A repercussão da adoção de programas de compliance de dados pessoais

Observadas as características constantes da LGPD, o *compliance* possui papel fundamental na garantia do cumprimento da legislação referente à proteção de dados pessoais[116]. Além disso, a adoção de boas práticas de governança corporativa auxilia na construção de uma relação de confiança com o titular dos dados por meio de uma atuação transparente que é vista como um diferencial competitivo nos negócios[117].

Há que se concordar com Frazão, Oliva e Abilio na afirmação de que implementação dos programas de *compliance* demonstram que o tratamento de dados pessoais está sendo realizado de forma regular pelos agentes de tratamento, podendo, inclusive, servir como isenção de responsabilidade civil[118]. Além disso, a adoção de políticas de boas práticas e governança,

[115] Ibidem. p. 694.
[116] Ibidem. p 693.
[117] Ibidem. p 478.
[118] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p 711.

inclusos os programas de *compliance*, são um critério atenuante no momento da definição da sanção por eventual descumprimento[119].

Assim, nota-se que o *compliance* de dados pessoais visa auxiliar os agentes de tratamento a aplicar as normas de proteção de dados de forma eficaz e, por isso, acaba por conduzir a organização à uma conformidade legal, utilizando a segurança da informação para diminuir incidentes que resultem na responsabilidade empresarial[120].

Depois de expostas as informações acima sobre a governança corporativa e o compliance, é preciso demonstrar como se dá o funcionamento das investigações internas realizadas por esses programas quando da apuração de possíveis atos ilícitos percebidos pela empresa, conforme será exposto a seguir.

4.3.2 *Investigações internas de programas de compliance infracional*

De início, é necessário evidenciar o funcionamento das investigações internas de programas de *compliance*. Ela pode ser iniciada de várias formas, sendo a mais comum a denúncia. Conforme o relatório da Associação de Examinadores Certificados de Fraudes (ACFE)[121], 40% das fraudes investigadas em uma empresa decorrem de denúncias realizadas por funcionários ou terceiros. Além disso, as investigações também podem ser iniciadas após realização de auditoria interna. Pode ocorrer, também, investigação externa que pode acabar motivando o início de uma investigação interna.

Fato é que, depois de percebido algum indício de problema ou recebida denúncia, deve-se iniciar uma investigação interna de *compliance*. Tais processos podem ser realizados por profissionais especializados ou por uma equipe da empresa ou terceirizada. É importante que haja isenção de interesses e confiança nas pessoas que realizarão a investigação. Depois de definida a equipe, deve ser feito um plano de ação para a investigação, contando com: *(i)* os passos necessários; *(ii)* as perguntas a serem feitas; *(iii)* o motivo do processo; *(iv)* as hipóteses levantadas; e *(v)* as pessoas a serem entrevistadas, sejam testemunhas ou investigados[122].

---

[119] BLUM, Rita Peixoto Ferreira; MORAES, Helio Ferreira. Lei Geral de Proteção de Dados Pessoais - LGPD. *In*: CARVALHO, André Castro *et. al*. Manual de *Compliance*. 2. ed. Rio de Janeiro: Forense, 2020. p. 510.
[120] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p 694.
[121] ACFE. Report to the Nations, 2020 global study on occupational fraud and abuse. Disponível em: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf. Acesso em: fevereiro de 2021.
[122] ACFE. Report to the Nations, 2020 global study on occupational fraud and abuse. Disponível em: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf. Acesso em: fevereiro/2021.

Os benefícios das investigações internas de *compliance* são percebidos a médio e longo prazo, ainda que inicialmente pareça melhor ocultar os problemas. Com esse processo, é possível evitar que a empresa sofra sanções legais e penais e/ou danos financeiros ou à imagem. Vale destacar que uma investigação pode não resultar em nenhuma conclusão ou denúncia. Entretanto, apenas a desconfiança de um problema já justifica o início do processo.

Sendo assim, uma vez motivado o início da investigação, esta deve ser realizada da melhor forma possível. O resultado sempre será benéfico para empresa visto que pode apontar um problema ou uma falha, oportunidade em que podem ser realizadas melhorias. Diante do exposto, é importante frisar que as investigações devem ser realizadas de modo a manter a rotina da empresa, da forma mais natural possível, e deve ser tida como algo natural.

Dentre os critérios que devem ser observados quando da realização de investigações internas, o principal é a confidencialidade. Posto isso, apenas os responsáveis pelos canais de denúncias e os investigadores devem saber as fontes das informações. Isso ocorre para evitar que as pessoas envolvidas escondam ou destruam provas e/ou evidências, podendo haver até ameaças a testemunhas, atrapalhando o processo. Ademais, o sigilo visa proteger a imagem dos investigados, dos denunciantes e da própria empresa.

No entanto, as informações estão sujeitas a vazamento a todo momento, podendo causar medo nos funcionários em realizar denúncias e nas possíveis punições que podem vir a sofrer. Para evitar essa situação, é essencial possuir um programa de *compliance* que conte com profissionais especializados, visto que isso garantirá os recursos e meios necessários para o processo.

Destacam-se, resumidamente, alguns pontos já expostos para a devida realização de investigações internas de *compliance*, de forma a respeitar a privacidade e proteger os dados pessoais dos envolvidos: *(i)* não pode ser investigada a vida pessoal e a privacidade das pessoas; *(ii)* deve existir justo motivo para o início do processo – denúncia e/ou apontamento em auditoria interna; *(iii)* todos os equipamentos, sistemas e infraestrutura da empresa podem ser utilizados, desde que não haja expectativa de privacidade quanto a eles; e *(iv)* todos os meios para garantir o sigilo e o tempo necessário para a investigação devem ser fornecidos pela empresa[123].

Depois de analisado o funcionamento das investigações internas realizadas por programas de *compliance* quando da apuração de possíveis atos ilícitos percebidos pela

[123] ACFE. Report to the Nations, 2020 global study on occupational fraud and abuse. Disponível em: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf. Acesso em: fevereiro/2021.

empresa, de modo a garantir a privacidade e a proteção de dados dos envolvidos, faz-se necessário analisar com maior profundidade a relação entre a LGPD, os programas de compliance e as investigações internas, conforme será realizado a seguir.

4.3.3 A relação entre a LGPD, os programas de compliance e as investigações internas

Para analisar a relação entre a LGPD, os programas de compliance e as investigações internas, será abordado, inicialmente, como se dá a implementação da LGPD nas empresas por seus programas de compliance, bem como sua relação direta.

4.3.3.1 A implementação da LGPD pelos programas de compliance

A lei deixa a cargo das organizações os investimentos relativos à segurança tecnológica para impedir violações aos dados pessoais[124]. Soma-se à essa outras obrigações das empresas para implementação da LGPD, como o mapeamento criterioso das atividades de cada departamento interno no que se refere à coleta e ao tratamento de dados pessoais, a fim de obter uma lista de ações específicas para cada departamento e proporcionar o atendimento dos requisitos da lei. Por fim, há a implantação propriamente dita.

Com a implantação da LGPD, toda e qualquer empresa que lide direta ou indiretamente com dados pessoais externos à organização deverá ter um controle e uma gestão desses dados, para que estejam em conformidade com a lei, desde os dados de visitantes, prestadores de serviços, clientes e stakeholders. Nesse último caso, as exigências da lei abrangem todas as empresas. Dessa forma, é essencial que as empresas busquem adequar práticas e gestão de dados para que estejam em *compliance* com as exigências da LGPD.

Surge, então, uma dúvida geral: como implementar a LGPD nas organizações? Para isso, é necessária a reestruturação e readequação dos processos internos – por meio da Governança Corporativa e seus programas - que envolvam dados de terceiros em 6 passos, quais sejam: *(i)* identificar os agentes envolvidos; *(ii)* identificar os dados essenciais; *(iii)* garantir o consentimento na coleta dos dados; *(iv)* garantir a conformidade dos fornecedores; *(v)* definir um responsável na empresa; e *(vi)* obter apoio legal.

[124] ROCHA, Camila P D et al. Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, v. 2, n. 3, p. 78-97, 2019.

A priori, para que sejam identificados os dados essenciais, deve-se observar todos os agentes envolvidos na lei, conforme já exposto: o titular, o controlador, o operador e o encarregado pelos dados. Além disso, deve-se observar quais momentos a empresa atua como controlador de dados e quais as ferramentas são utilizadas para isso – ou quais empresas contrata para exercer essa função. Ainda, é importante identificar os tipos de titulares que a empresa tem contato, sendo necessário até mesmo suporte legal para essa tarefa, diante da multiplicidade de fontes de dados e a dificuldade em realizar essa etapa.

Em seguida, é necessário identificar quais são os dados essenciais que a empresa precisa coletar de seus titulares. Não há como negar a importância da coleta de dados para as empresas, seja estrategicamente para crescimento de vendas ou mesmo segurança. Entretanto, não devem ser coletados mais dados do que o necessário para a execução de estratégias e para garantir a segurança da empresa. Por isso, é importante listar os dados necessários para que sejam mapeados com segurança, de forma a identificar as mudanças necessárias nos processos internos para que seja garantido o *compliance*.

Em terceiro lugar, é preciso garantir o consentimento para que seja realizada a coleta de dados. Sendo esse um pilar da LGPD, é obrigatório evidenciar o consentimento do titular com a coleta dos dados, seja por meio de cláusula, termo ou alguma ferramenta. O usual "Li e aceito os termos de uso" já evidencia o consentimento. Além disso, é fundamental que a empresa realize o *compliance* dos seus dados e informações em relação a terceiros e implante um termo de confidencialidade para que seja garantida a proteção legal de seus dados.

Posteriormente, é preciso garantir a conformidade dos fornecedores pois, para a LGPD, não basta que apenas a empresa e seus processos estejam em conformidade com a gestão de dados. Isso porque alguns fornecedores exercem o papel de operadores dos dados e a empresa só deve trabalhar com fornecedores que também estejam em conformidade com a LGPD, sob pena de ser legalmente responsável por eventuais falhas e vazamentos de dados causados pelos fornecedores.

Devido a quantidade de dados de diversas naturezas, principalmente os dados coletados de forma virtual, é preciso, também, definir um responsável fixo na empresa para a função de encarregado. Nesse contexto, surgiu a necessidade de um *Data Protection Officer* (DPO) nas empresas, ficando responsável pela gestão e controle desses dados. Essa função tem sio cada vez mais valorizada nos departamentos de tecnologia da informação e empresas de tecnologia para que seja garantida uma boa gestão de dados e a adequação à LGPD.

Por fim, vale dizer que as empresas precisam de apoio legal para garantir que estejam em conformidade com a LGPD, seja interno ou externo. Especialistas conseguem observar os detalhes do negócio e identificar possíveis falhas na gestão de dados, nos processos internos, bem como nas alterações contratuais e documentos.

4.3.3.2 A relação entre a LGPD e os programas de compliance

Vistos os requisitos dos programas de *compliance* e como se dá a implementação da LGPD por eles, é preciso relacioná-los à Lei 13.709/2018, abordando as responsabilidades e sanções administrativas previstas. A LGPD prevê, em seu artigo 50 que os controladores e os operadores podem elaborar regras de boas práticas e de 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. [...][125]

Quando da elaboração das regras de boas práticas, as agentes de tratamento deverão analisar "[...] a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular"[126]. Ademais, poderá ser formulado, pelo controlador, programa de governança em privacidade, a depender da estrutura e volume das operações, bem como a sensibilidades dos dados e a possibilidade de gerar danos aos titulares. É importante ressaltar que o programa de governança em privacidade é previsto exclusivamente para o controlador e amplo, com elaboração de normas de governança corporativa. Enquanto as regras de boas práticas e governança tendem a se preocupar com questões operacionais relativas ao tratamento de dados[127].

Alguns requisitos do programa de governança em privacidade previstos no artigo 50 da LGPD são:

---

[125] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: fevereiro de 2020.
[126] Idem.
[127] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 701.

> [...] 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; [...][128].

O programa de governança em privacidade nada mais é do que o conjunto de regras de boas práticas e governança a serem utilizadas pelos agentes de tratamento de dados pessoais. É semelhante à política de segurança da informação, a diferença é que tem por objetivo cumprir ordens legais[129]. Além disso, está alinhado às políticas de governança e *compliance*, objetivando a realização da gestão de riscos para observância da lei e dos regulamentos internos[130].

Para um programa de *compliance* de dados pessoais, é necessário ter a ciência de todos os fluxos de dados existentes na organização, mapeando o ciclo de dados desde a forma de sua coleta até seu armazenamento, incluindo as principais caraterísticas[131]. É importante observar quais tipos de dados estão sendo tratados e se estão de acordo com as hipóteses legais que de tratamento. Novamente, percebidos os riscos, deve ser elaborado o Código de Conduta ou de Boas Práticas para tratar dos mecanismos do tratamento dos dados, contendo as instruções e os

---

[128] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: fevereiro de 2020.

[129] BLUM, Rita Peixoto Ferreira; MORAES, Helio Ferreira. Lei Geral de Proteção de Dados Pessoais - LGPD. *In*: CARVALHO, André Castro *et. al*. Manual de *Compliance*. 2. ed. Rio de Janeiro: Forense, 2020. p. 509; COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 198.

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

[131] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 699.

valores que servirão de guia para os funcionários e a alta administração nas decisões, além de incorporar ações previstas na política de privacidade e mencionar quais dados podem ser manuseados, em quais hipóteses de tratamento, para quais finalidades e o período autorizado recomendável de armazenamento[132].

Além do mais, deve prever, gradualmente, as medidas a serem realizadas, os mecanismos de alerta dos dados de acordo com seu grau de risco para o titular. Isso permite que os funcionários reconheçam e demonstrem mais cuidado nesses casos[133]. Ainda, "se possível, é interessante estabelecer quais funcionários estão autorizados a realizar coleta e tratamento de dados, bem como segmentar que funcionários podem acessar que espécie de informações", conforme explicam Frazão, Oliva e Abilio[134].

No Código de Conduta, ou na política de privacidade, deve constar claramente os cuidados que são adotados para a proteção dos dados e, em caso de falhas, os procedimentos que serão adotados para recuperação dos dados e notificação ao titular. Deve contar, também, os recursos disponíveis aos titulares na legislação e o encarregado pelo tratamento dos dados[135].

Uma das funções do programa de *compliance* é assegurar que o tratamento de dados permitirá o pleno exercício dos titulares, prezando pela transparência. Nesse sentido, para Frazão, Oliva e Abilio: "A participação do titular deverá influenciar na valoração positiva das normas de *compliance* pela ANPD, de modo que o envolvimento da sociedade civil na própria construção das normas corporativas e revisão da política de privacidade pode ser um relevante indício da robustez do programa"[136].

Conforme visto no capítulo 2, é essencial que sejam observados os princípios de segurança, confidencialidade e integridade dos dados armazenados[137]. Aqui, o apoio da alta administração é essencial. A depender dos riscos envolvidos e com base na capacidade na elaboração de práticas correspondentes a LGPD, a organização poderá contratar um encarregado pelo tratamento dos dados pessoais[138].

Para que seja garantida a segurança do programa de *compliance* de dados pessoais, este deve ser monitorado e atualizado constantemente, instaurando proteções aos possíveis impactos

---

[132] Ibidem. p. 700-702.
[133] Ibidem. p. 703.
[134] Ibidem.
[135] Ibidem. p. 705.
[136] Ibidem.
[137] Ibidem. p. 706.
[138] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 708.

e riscos à privacidade[139]. Desta maneira, devem ser promovidos treinamentos constantes para orientar os funcionários sobre as práticas de governança de proteção de dados pessoais, inclusive os que atuam com a tecnologia da informação.

Ainda, vale dizer que os programas de *compliance* e os Acordos de Leniência objetivam de combate à corrupção, aos atos ilícitos e às más práticas de conduta por parte das pessoas jurídicas, demonstrando interesse e compromisso em, futuramente, honrar com os compromissos de sua função social, garantindo, também, uma boa relação com o Estado e frente à sociedade.

Por fim, conforme exposto, para a implementação dos programas de *compliance* de dados pessoais, é preciso revisar e atualizar o termo de uso e a política de privacidade da organização, bem como das cláusulas de contratos com os parceiros que exercem alguma operação com os dados, o mapeamento do fluxo de dados pessoais, a atualização de tabela com os logs de consentimento, bem como da política de segurança da informação[140]. Isso comprova a importância das normas de governança determinadas na esfera das operações de tratamento de dados pessoais, a fim de que sejam bem estruturadas e supram às determinações da legislação[141].

[139] Ibidem. p. 709.
[140] PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018, p. 45-47.
[141] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 698.

5 CONCLUSÕES

Consoante o exposto no primeiro capítulo, que objetiva identificar um potencial choque entre o direito à privacidade de dados e o interesse legítimo das empresas, serão agrupadas as conclusões realizadas. Inicialmente, vale destacar que, no âmbito das relações de trabalho, a autodeterminação informativa (um dos fundamentos da LGPD) visa limitar o poder diretivo do empregador quanto à coleta, distribuição e armazenamento de dados do trabalhador.

Na sequência, a intimidade foi conceituada como a parte mais reservada do indivíduo restrita a apenas ele, enquanto a privacidade corresponde a atos humanos externos do indivíduo de conhecimento seleto, limitado ao desejo do indivíduo de divulgá-las. Dito isso, a proteção de dados, grosso modo, é a forma de garantir a possibilidade de os cidadãos determinarem individualmente a utilização de seus dados pessoais e evitar que o mau uso cause quaisquer danos.

Devido ao caráter da LGPD de proteger os direitos fundamentais, indispensáveis à manutenção da dignidade da pessoa humana, no que se refere a atividades que envolvam dados pessoais, esses direitos podem colidir com os direitos fundamentais de outros particulares, como no caso do direito à privacidade dos empregados e o poder diretivo do empregador, cumprindo com o objetivo deste capítulo de identificar se, de fato, se confirmaria tal choque entre direitos.

Entretanto, devem ser observados os seguintes requisitos elencados no artigo 10 da LGPD para que seja aplicado o teste de proporcionalidade do legítimo interesse: *(i)* a verificação da legitimidade do interesse por parte do controlador dos dados; *(ii)* a necessidade do uso dos dados coletados; *(iii)* o balanceamento entre a obtenção de dados pelo controlador e a disponibilização do dado pelo titular; e *(iv)* a transparência do procedimento e da finalidade dos dados coletados com o titular e os mecanismos de diminuição de riscos. Esses requisitos devem ser preenchidos para que este instituto seja utilizado.

Além do mais, são os direitos da intimidade, da honra, da imagem, de liberdade, da livre iniciativa e do desenvolvimento econômico e tecnológico que orientam a proteção da dignidade e da personalidade humana, sendo o direito à privacidade o mais importante, já que é tido como um reflexo da personalidade humana, fundamentado pela proteção da dignidade.

Diante dos reflexos decorrentes da interposição das questões relativas ao direito à privacidade e aos direitos fundamentais, expostas acima, quando do uso do legítimo interesse para a celebração de acordos de cooperação com a administração pública, apesar de o

consentimento e os contratos serem as duas principais bases legais da LGPD, o legítimo interesse é uma das mais relevantes, devido ao seu caráter flexível. Esta base legal, por sua vez, se mostrou como uma medida capaz de flexibilizar as relações de dados na Europa e no Brasil.

É importante ressaltar que, quando percebida a conduta ilícita praticada por funcionário da empresa, seja por meio de denúncia ou de auditoria, cabe à empresa tomar as devidas precauções para que não sejam cometidos mais atos do tipo, as medidas necessárias para seu reparo e, ainda, promover denúncia à autoridade competente pela fiscalização. Nessa oportunidade, há a possibilidade de ser realizado acordo de cooperação entre a empresa e a administração pública, foco dado a este trabalho. No entanto, as conclusões da pesquisa se aplicam também para a promoção de denúncia à autoridade competente, por parte da empresa, no que tange à utilização de dados pessoas de funcionários.

Contudo, surgem algumas questões, ainda sem resposta: o trabalhador tem dever de denunciar uma ilicitude que vivenciou? O trabalhador pode ficar em silêncio diante de uma investigação interna? Quem sabe futuros estudos responsam à esses e outros questionamentos.

Quanto aos requisitos para celebração destes acordos e as novas diretrizes da LGPD aplicáveis às investigações internas, tratados no capítulo 2, depreende-se que a proteção de dados é a forma de garantir a possibilidade de os cidadãos determinarem individualmente a utilização de seus dados pessoais e evitar que sejam causados quaisquer danos. No entanto, quando os direitos fundamentais e de privacidade colidirem com os direitos fundamentais de outros particulares, como no caso do direito à privacidade dos empregados e o poder diretivo do empregador, deve ser analisado caso a caso.

Já no que tange à celebração de acordos de cooperação, são 5 os requisitos gerais para a celebração de acordos, quais sejam: *(i)* a manifestação de interesse em cooperar para a apuração de ato lesivo específico, quando tal circunstância for relevante; *(ii)* a cessação da prática da irregularidade investigada; *(iii)* a cooperação com as investigações, identificando os demais envolvidos na infração quando couber; *(iv)* o fornecimento de informações e documentos que comprovem a infração; e *(v)* o comprometimento de implementar ou melhorar mecanismos internos de integridade (*compliance*), auditoria, incentivo às denúncias de irregularidades e à aplicação efetiva de código de ética e de conduta na organização.

A fim de mapear os limites de natureza, coleta e uso de dados pessoais definidos na LGPD, inicialmente, no capítulo 2, foi tratada a diferenciação entre dados pessoais, que são informações pertencentes a alguém que podem ser relacionadas a identificação ou possibilitar

a identificação de alguém, de modo individualizado, e sensíveis, que podem dar margem para alguma discriminação ou preconceito, podendo comprometer a privacidade do indivíduo.

Quanto à coleta de dados pessoais, é importante destacar que devem ser coletados apenas os dados que forem essenciais para a segurança e/ou gestão da empresa. Sendo assim, não devem ser coletados dados que não possuem uma finalidade concreta, e esse requisito deve ser observado principalmente quanto aos dados sensíveis.

No entanto, a LGPD prevê o consentimento do titular dos dados pessoais para que haja seu tratamento. Para isso, não basta que seja dada autorização quando da coleta dos dados, mas, sim, que seja garantido ao titular conhecimento de como seus dados serão tratados e para qual finalidade. A autorização de tratamento em função de consentimento deve ser livre, informada e inequívoca, não havendo consentimento do titular quando este permanecer em silêncio. Contudo, há exceções.

Dentre as possibilidades tratadas que permitem o tratamento de dados sem o consentimento do titular, a mais relevante para esta pesquisa é a base legal do legítimo interesse do controlador, excetuando-se os casos em que prevalecem direitos e liberdades fundamentais do titular que exijam a proteção desses dados. Vale destacar que não há definição de um limite claro por parte da legislação quando se envolve o tratamento de dados por legítimo interesse de terceiro.

Vale ressaltar, ainda, que no Brasil convencionou-se que apenas os portadores de CPF são titulares de dados, conforme a LGPD, ao passo que portadores de CNPJ não. Contudo, se houver fato explícito que comprove a má conduta do funcionário, poderá ser desnecessário o consentimento do titular para uso dos dados, devendo ser respeitados os limites para garantir a proteção de dados do funcionário.

Apesar de não ser requisitado consentimento do titular em alguns casos, restam guardados os demais direitos, como o de informação. Sendo assim, não são dispensados os deveres dos agentes de tratamento elencados na lei. O operador, no que lhe diz respeito, a lei considera ser responsável por processar dados pessoais em nome do controlador. Quem determina os termos do tratamento de dados é o controlador, e quem executa é o operador. Sendo assim, a principal responsabilidade deles é garantir a segurança desses dados, dos meios utilizados para transferi-los de uma organização para outra e das ferramentas aplicadas para recuperá-los, ou seja, que seja realizado o devido tratamento de dados pessoais em todas as suas etapas.

Dessa forma, é estabelecida uma relação de confiança entre o titular dos dados e o controlador, que possui elevado potencial de dano caso não seja realizado o devido tratamento. Se o titular autoriza a coleta, uso e tratamento dos seus dados, é porque há uma relação de confiança de que eles serão bem tratados, sem prejuízos, além da predominância do princípio da boa-fé por parte dos agentes de tratamento. Mas se o controlador utiliza esses dados, sem o consentimento do titular, sabendo ou com a finalidade de lhe causar prejuízo, mesmo que em sua defesa, essa seria uma violação aos direitos dos titulares. Ora, não é natural que alguém em sã consciência tome decisões esperando ser prejudicado por estas, ou seja, autorizar a coleta, uso e tratamento de seus dados se achar que será prejudicado.

Percebe-se, isto posto, que não há mais espaço para coleta e tratamento de dados pessoais sem finalidade relevante para o cidadão e, na maioria das vezes, sem consentimento, excluindo-se as exceções. É necessário que o cidadão se torne realmente dono de suas próprias informações e de seus dados, especialmente nas ocasiões em que o consentimento é necessário, de forma a evitar que o aceite não seja algo meramente proforma, ajustando o mercado a esse novo formato de tratamento de dados pessoais.

É importante ressaltar que, apesar do foco dado na base legal do consentimento, a fim de equilibrar a relação empregado-empregador, ainda deve ser estudada a base legal do cumprimento legal - infelizmente não foi possível neste trabalho.

Dentre as atribuições e responsabilidades abordadas, cabe destacar a aplicação do princípio da boa-fé cabíveis exclusivamente ao controlador, e, eventualmente, ao operador. Além do mais, fica evidenciado que os dados pessoais podem ser tratados para atender aos interesses legítimos do controlador ou de terceiros, excetuando-se os casos em que prevalecem direitos e liberdades fundamentais do titular que exijam a proteção desses dados. Apesar de não haver definição de um limite claro por parte da legislação quando se envolve o tratamento de dados por legítimo interesse de terceiro, restam guardados os demais direitos do indivíduo.

A LGPD traz um viés pedagógico e punitivo, deixando de lado o indenizatório e, considerando que a ANPD acumula grande parte das funções de fiscalizar, investigar e garantir a segurança do disposto na lei, deve haver o quanto antes a estruturação desse órgão para garantir a eficácia prática da LGPD.

Percebe-se, desta maneira, a necessidade de cumprir com o princípio da finalidade, devendo todo e qualquer ato de utilização de dados pessoais ser informado ao seu titular. Soma-se a isso a obrigatoriedade de os agentes de tratamento comunicarem aos titulares dos dados caso haja alguma violação de segurança.

Conforme exposto, não há dúvidas quanto à necessidade de tutela da privacidade em relação aos dados. Esse movimento tem se tornado uma tendência mundial, e pode ser confirmado pela decisão do Tribunal de Justiça da União Europeia ao condenar o Google a apagar dos resultados de buscas links associados a pessoas dependendo da natureza da informação e da gravidade para a vida privada.

Justamente pelo impacto que o não cumprimento do direito de eliminar os dados pessoais pode causar sobre a atividade econômica desempenhada pelos agentes de tratamento e os direitos fundamentais dos envolvidos, é percebida a necessidade de assegurar ao titular dos dados o direito de não permanecer vinculado a informações inverídicas, incompletas ou que se tornem irrelevantes, que está intimamente ligado ao direito de exclusão de dados.

Dessa forma, resumidamente, fica evidente que devem ser observadas as etapas de proteção de dados, levando-se em conta: *(i)* sua natureza, que definirá o grau de proteção a ser dado; *(ii)* a coleta e armazenamento apenas dos dados que forem essenciais para a segurança e/ou gestão da empresa; *(iii)* o princípio da finalidade, que determina que todo e qualquer ato de utilização de dados pessoais deve ser informado ao seu titular; e *(iv)* a eliminação eficaz dos dados após o término do seu uso.

Aqui, vale lembrar algumas perguntas realizadas no capítulo 1: *(i)* quais são os requisitos definidos pela LGPD para que a empresa possa utilizar dados de trabalhadores obtidos em investigações internas de *compliance* para a celebração de acordos com a administração pública quando tal trabalhador não é colaborador do acordo; e *(ii)* se os dados pessoais coletados pelas empresas, seja rotineiramente ou por meio de investigações internas realizadas por seus programas de *compliance*, podem ser utilizados para atender ao interesse dela quando da celebração de acordos com a administração pública.

Diante do exposto, conclui-se que devem ser cumpridas quatro fases para se verificar o devido preenchimento do requisito do legítimo interesse para fins de que seja possível o uso de informações e documentos dos funcionários para a celebração de AL, quais sejam: *(i)* a avaliação dos interesses legítimos; *(ii)* o impacto sobre o titular do dado; *(iii)* o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e *(iv)* as salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado.

No entanto, restam questionamentos, a ser respondidos em outra oportunidade, como: em que medida um bom programa de *compliance*, inclusive um que dite as "regras do jogo", define quais dados podem ser coletados dos funcionários para fins específicos? A LGPD mudou

a forma das empresas monitorarem os empregados? Quais as legitimas expectativas do empregado em termos de privacidade?

Depreende-se, portanto, que os dados pessoais coletados pelas empresas, seja rotineiramente ou por meio de investigações internas realizadas por seus programas de *compliance*, podem ser utilizados para atender ao legitimo interesse da empresa quando da celebração de acordos com a administração pública, desde que cumpridos os requisitos apresentados.

No entanto, contrariamente do verificado no teor dos julgados colacionados, ainda no capítulo 2, cumpre defender que a coleta e o tratamento indevido de dados pessoais deve ser um fator que caracteriza um autêntico dano, não sendo necessária a comprovação de um prejuízo concreto para ser caracterizada a responsabilidade civil. O fato de uma empresa permitir, ainda que culposamente, que terceiro, estranho e desconhecido, tenha acesso a informações pessoais, privadas e/ou íntimas caracteriza um dano, correspondente à violação à privacidade e, em alguns casos, da intimidade dos indivíduos lesados.

Por todo o exposto é que se fez necessário estudar e expor claramente quais são os requisitos e os trâmites que devem ser cumpridos, em cumprimento à LGPD, para que sejam realizadas investigações internas dos programas de *compliance* e celebrados acordos de cooperação com a administração pública. Principalmente para proteger a privacidade, a intimidade e os dados pessoais dos indivíduos envolvidos, bem como sejam observados os princípios de segurança, confidencialidade e integridade dos dados armazenados, de acordo com o exposto ao longo da pesquisa.

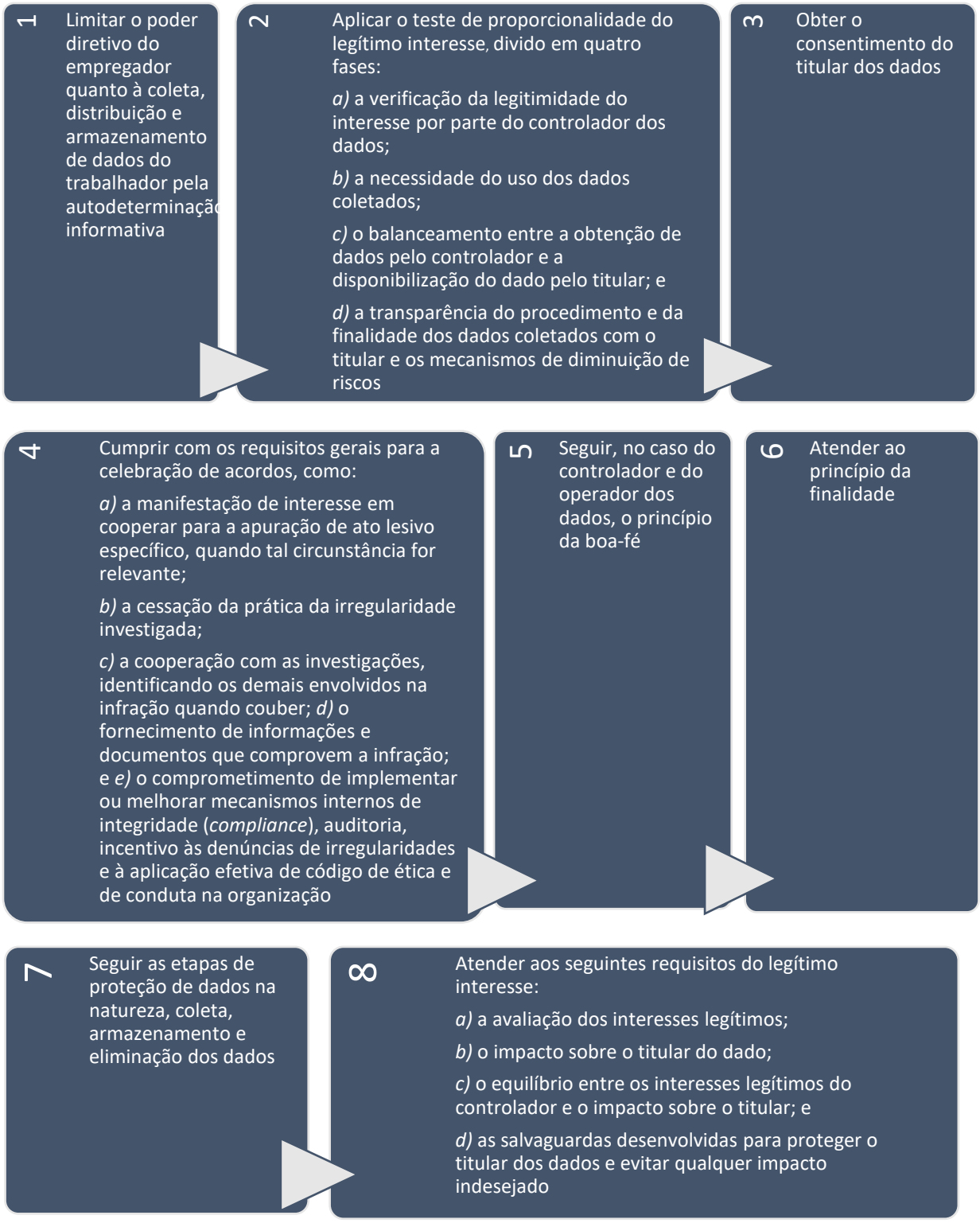
Consoante apresentado no capítulo 4, para a implementação dos programas de *compliance* de dados pessoais, é preciso, também, revisar e atualizar o termo de uso e a política de privacidade da organização, bem como da política de segurança da informação, e as cláusulas de contratos com os parceiros que exercem alguma operação com os dados. Soma-se a isso o mapeamento do fluxo de dados pessoais e dos devidos consentimentos dos titulares. Vale repetir que isso comprova a importância das normas de governança determinadas na esfera das operações de tratamento de dados pessoais, a fim de que sejam bem estruturadas e supram às determinações da legislação.

Vale ressaltar que o apoio da alta administração é essencial para bons resultados, principalmente, para que seja garantida a segurança do programa de *compliance* de dados pessoais, que deve ser monitorado e atualizado constantemente, instaurando proteções aos possíveis impactos e riscos à privacidade dos envolvidos. Ademais, devem ser promovidos

treinamentos constantes para orientar os funcionários sobre as práticas de governança de proteção de dados pessoais, inclusive os que atuam com a tecnologia da informação.

Diante do exposto, depreende-se também que, para que seja possível cumprir com os requisitos para celebração dos acordos e gozar dos benefícios acordados, a empresa deve expor diversos dados pessoais dos envolvidos. Fato é que, até a LGPD, não havia preocupação com quais dados eram expostos, em que circunstâncias, como se dava o tratamento, armazenamento e exclusão desses dados. Agora, devem ser observados os requisitos dispostos para garantir a proteção dos dados pessoais, quais sejam: *(i)* limitar o poder diretivo do empregador quanto à coleta, distribuição e armazenamento de dados do trabalhador pela autodeterminação informativa; *(ii)* aplicar o teste de proporcionalidade do legítimo interesse, dividido em quatro fases: *a)* a verificação da legitimidade do interesse por parte do controlador dos dados; *b)* a necessidade do uso dos dados coletados; *c)* o balanceamento entre a obtenção de dados pelo controlador e a disponibilização do dado pelo titular; e *d)* a transparência do procedimento e da finalidade dos dados coletados com o titular e os mecanismos de diminuição de riscos; *(iii)* obter o consentimento do titular dos dados; *(iv)* cumprir com os requisitos gerais para a celebração de acordos, como: *a)* a manifestação de interesse em cooperar para a apuração de ato lesivo específico, quando tal circunstância for relevante; *b)* a cessação da prática da irregularidade investigada; *c)* a cooperação com as investigações, identificando os demais envolvidos na infração quando couber; *d)* o fornecimento de informações e documentos que comprovem a infração; e *e)* o comprometimento de implementar ou melhorar mecanismos internos de integridade (*compliance*), auditoria, incentivo às denúncias de irregularidades e à aplicação efetiva de código de ética e de conduta na organização; *(v)* seguir, no caso do controlador e do operador dos dados, o princípio da boa-fé; *(vi)* atender ao princípio da finalidade; *(vii)* seguir as etapas de proteção de dados na natureza, coleta, armazenamento e eliminação dos dados; e *(viii)* atender aos seguintes requisitos do legítimo interesse: *a)* a avaliação dos interesses legítimos; *b)* o impacto sobre o titular do dado; *c)* o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e *d)* as salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado.

Para melhor entendimento, observe o esquema abaixo:

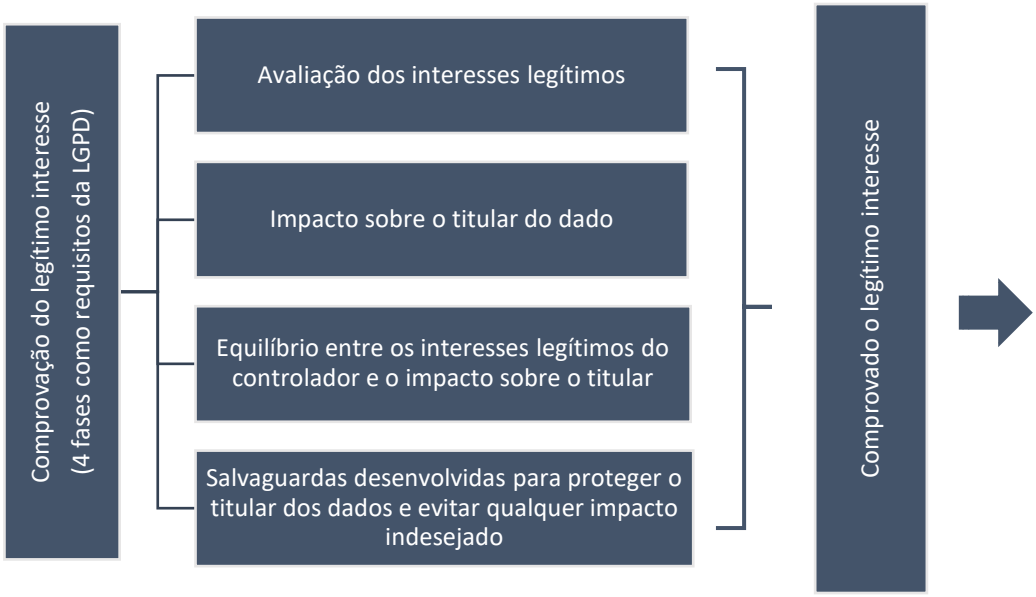


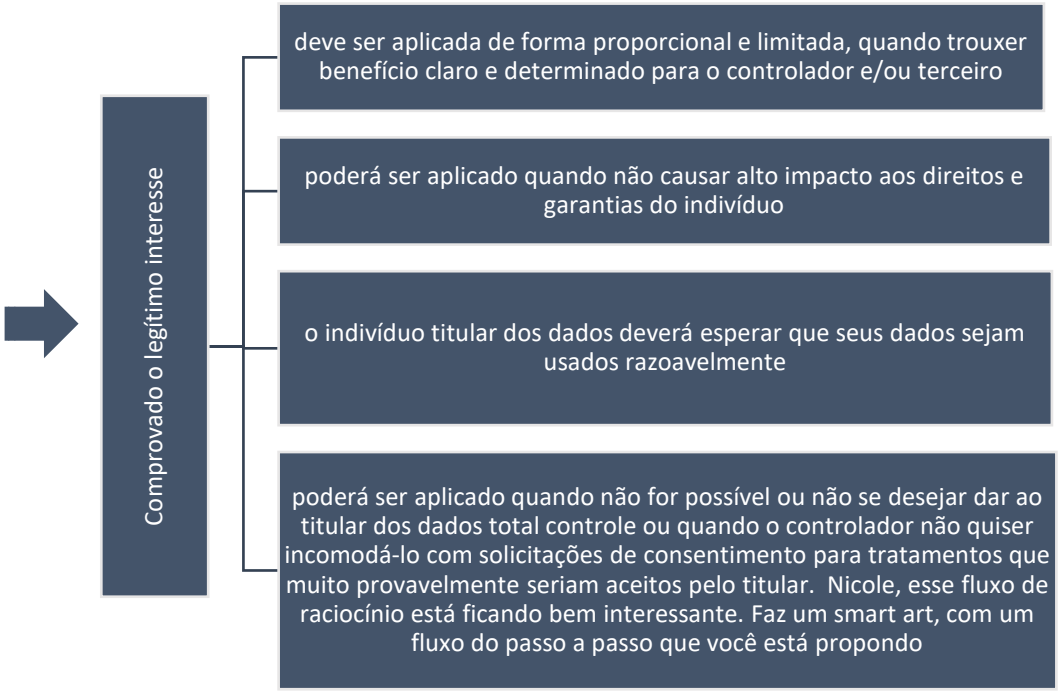
Elaborado pela autora.

A procura por caminhos alternativos com menores punibilidades têm aumentado cada vez mais. Os benefícios que podem ser concedidos às empresas, pessoas físicas e jurídicas são atrativos e podem estimular a ultrapassagem de limites relativos aos direitos dos envolvidos, ou

não, em práticas ilícitas. Diante da variedade de acordos existentes, é proposto que sejam mapeados os limites de natureza, coleta, uso, armazenamento e exclusão de dados pessoais definidos na LGPD, conforme foi exposto no capítulo 3, devido ao alto número de pessoas que podem ser afetadas em investigações internas para verificação de tais práticas ilícitas objetivando a celebração de acordos.

Ademais, diante do exposto ao longo do capítulo 4 e a fim de elencar os requisitos necessários para uso de dados pessoais oriundos de investigações internas nos acordos com a administração pública, conclui-se que o legítimo interesse: *(i)* pode ser a base legal mais apropriada em diversas hipóteses, devendo, no entanto, ser aplicada de forma proporcional e limitada, quando trouxer benefício claro e determinado para o controlador e/ou terceiro; *(ii)* poderá ser aplicado quando não causar alto impacto aos direitos e garantias do indivíduo; *(iii)* o indivíduo titular dos dados deverá esperar que seus dados sejam usados razoavelmente; e *(iv)* poderá ser aplicado quando não for possível ou não se desejar dar ao titular dos dados total controle ou quando o controlador não quiser incomodá-lo com solicitações de consentimento para tratamentos que muito provavelmente seriam aceitos pelo titular. Para melhor entendimento, o fluxo descrito está exemplificado abaixo:





Elaborado pela autora.

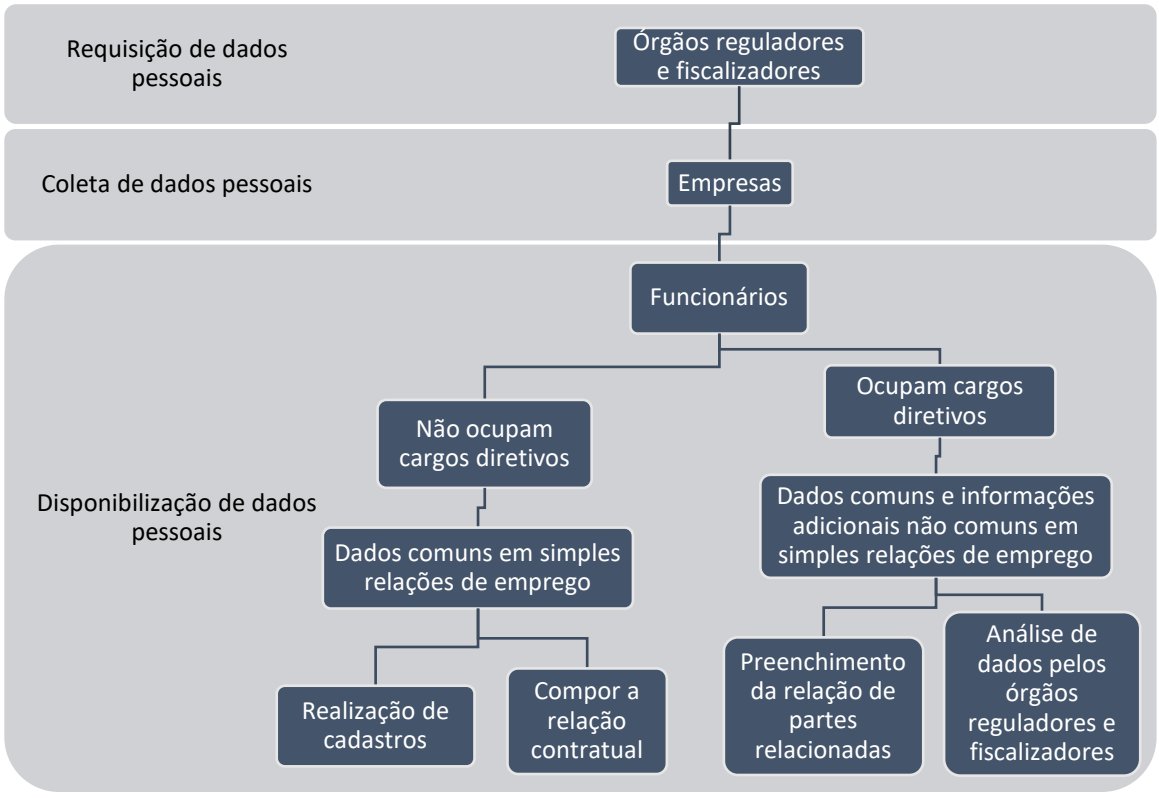
Sendo o devido consentimento dos titulares dos dados um dos requisitos mais importantes, ele deve ser observado para cumprimento da LGPD. Assim, para que sejam respeitadas as diretrizes da LGPD quando da celebração de acordos de cooperação, deve haver o prévio consentimento dos funcionários para que seus dados sejam tratados e utilizados para tal finalidade.

Em síntese, o consentimento na LGPD, para não configurar vício de vontade e ser considerado nulo, deve ser: *(i)* livre; *(ii)* informado; *(iii)* inequívoco; e *(iv)* com finalidade determinada. Para ser livre, o titular deve ter controle sobre o tratamento de seus dados pessoais, podendo escolher quais dados quer fornecer e retirar seu consentimento a qualquer momento. No entanto, deve-se apartar o consentimento de dados essenciais dos não essenciais, ficando a cargo do titular autorizar o uso de dados pessoais não obrigatórios para determinado fim, como no caso de celebração de acordos de cooperação com a administração pública em que não queira colaborar, caso em que apenas os dados necessários para a preenchimentos de cadastros e obrigações trabalhistas podem ser considerados obrigatórios.

Depreende-se, assim, que o instituto do consentimento possibilita ao titular condições de escolher produtos ou serviços que coletem seus dados pessoais, podendo dar consentimento específico para determinado tipo de tratamento e não para os outros pretendidos pelo controlador ou operador. Além disso, o titular pode revogar o seu consentimento a qualquer tempo.

No entanto, no caso dos funcionários de empresas que venham a celebrar acordos de cooperação, há que de destacar que os dados de diferentes funcionários são exigidos e monitorados em diferentes graus, dependendo do cargo que exercem, como conselheiros, diretores e demais funcionários. Nesse caso, os dados pessoais necessários, obrigatórios ou não, devem ser distintos.

Para os funcionários que não exercem cargos diretivos, devem ser coletados apenas os dados pessoais considerados comuns para realização de cadastros e compor a relação contratual, como nome completo, endereço, comprovante de residência, CPF, telefone, nome dos pais, endereço eletrônico, informações dos filhos e dependentes. No caso dos funcionários que exercem cargos diretivos, como diretores e conselheiros, são solicitadas informações adicionais não comuns em simples relações de emprego, como os dados para preenchimento da relação de partes relacionadas, para verificação do cumprimento dos requisitos de ocupação de cargos e outros citados no capítulo 3. Apesar da não obrigatoriedade de todos os tipos de empresas de instituírem políticas que regulem as relações com as partes relacionados de dirigentes, a maioria a implanta, apesar da escassa doutrina a respeito da matéria. Para melhor entendimento, o fluxo descrito está exemplificado abaixo:



Elaborado pela autora.

Assim, há um maior nível de exposição por parte dos funcionários que exercem funções diretivas nas entidades e, apesar de não haver legislação que regule a tipo das informações que podem ser solicitadas, a fim de que tais funcionários sejam resguardados e não tenham que fornecer informações pessoais desnecessárias, as empresas devem realizar uma análise interna e elencar quais informações são necessárias para atender às solicitações dos órgãos reguladores e, eventualmente, questioná-los sobre a real necessidade daquela informação.

Conclui-se, também, que a governança corporativa é uma estratégia ampla que engloba o programa de *compliance* – estratégia mais específica que a permite atingir seus objetivos, enquanto, por sua vez, o programa de *compliance* engloba o programa de integridade - estratégia mais específica ainda que o permite atingir seus objetivos, também. Conforme visto, devido a importância do *compliance*, é necessário avaliar os requisitos necessários para garantir a eficácia destes programas.

Conforme exposto, dentro dos programas de *compliance* podem existir subáreas específicas, como o *compliance* de dados pessoais, muito relevante no contexto dessa pesquisa. Dentre elas, nota-se que o compliance de dados pessoais visa auxiliar os agentes de tratamento a aplicar as normas de proteção de dados de forma eficaz e, por isso, acaba por conduzir a organização à uma conformidade legal, utilizando a segurança da informação para diminuir incidentes que resultem na responsabilidade empresarial.

Quando da apuração de possíveis atos ilícitos percebidos pela empresa, destacam-se, resumidamente, alguns pontos já expostos para a devida realização de investigações internas de *compliance*, de forma a respeitar a privacidade e proteger os dados pessoais dos envolvidos: *(i)* não pode ser investigada a vida pessoal e a privacidade das pessoas; *(ii)* deve existir justo motivo para o início do processo – denúncia e/ou apontamento em auditoria interna; *(iii)* todos os equipamentos, sistemas e infraestrutura da empresa podem ser utilizados, desde que não haja expectativa de privacidade quanto a eles; e *(iv)* todos os meios para garantir o sigilo e o tempo necessário para a investigação devem ser fornecidos pela empresa.

Além disso, é preciso garantir a conformidade dos fornecedores pois, para a LGPD, não basta que apenas a empresa e seus processos estejam em conformidade com a gestão de dados. Isso porque alguns fornecedores exercem o papel de operadores dos dados e a empresa só deve trabalhar com fornecedores que também estejam em conformidade com a LGPD, sob pena de ser legalmente responsável por eventuais falhas e vazamentos de dados causados pelos fornecedores.

Devido a quantidade de dados de diversas naturezas, principalmente os dados coletados de forma virtual, é preciso, também, definir um responsável fixo na empresa para a função de encarregado. Nesse contexto, surgiu a necessidade de um *Data Protection Officer* (DPO) nas empresas, ficando responsável pela gestão e controle desses dados. Essa função tem sido cada vez mais valorizada nos departamentos de tecnologia da informação e empresas de tecnologia para que seja garantida uma boa gestão de dados e a adequação à LGPD.

Por fim, vale dizer que as empresas precisam de apoio legal para garantir que estejam em conformidade com a LGPD, seja interno ou externo. Especialistas conseguem observar os detalhes do negócio e identificar possíveis falhas na gestão de dados, nos processos internos, bem como nas alterações contratuais e documentos.

Para que seja garantida a segurança do programa de *compliance* de dados pessoais, este deve ser monitorado e atualizado constantemente, instaurando proteções aos possíveis impactos e riscos à privacidade. Desta maneira, devem ser promovidos treinamentos constantes para orientar os funcionários sobre as práticas de governança de proteção de dados pessoais, inclusive os que atuam com a tecnologia da informação.

Por fim, conforme exposto, para a implementação dos programas de *compliance* de dados pessoais, é preciso revisar e atualizar o termo de uso e a política de privacidade da organização, bem como das cláusulas de contratos com os parceiros que exercem alguma operação com os dados, o mapeamento do fluxo de dados pessoais, a atualização de tabela com os logs de consentimento, bem como da política de segurança da informação. Isso comprova a importância das normas de governança determinadas na esfera das operações de tratamento de dados pessoais, a fim de que sejam bem estruturadas e supram às determinações da legislação.

Nesse contexto de proteção aos dados pessoais e sensíveis, é necessário dedicar atenção para a proteção humana da pessoa-trabalhadora, como um novo direito fundamental que garante aos seus titulares a capacidade de dispor de seus dados e controlar o uso que deles é feito, conforme visto no capítulo 1. Por isso, foi preciso avaliar os princípios que norteiam o tratamento dos dados e de que forma eles podem ser aplicados nas relações laborais a fim de assegurar aos trabalhadores uma proteção adequada. Além disso, tem-se que a proteção aos dados é um direito fundamental da pessoa-trabalhadora, ao passo que seus dados configuram expressão direta da própria personalidade.

Nesse sentido, espera-se que tenha sido encontrada uma resposta íntegra e coerente relativa à harmonização do conflito percebido entre o direito à privacidade e o interesse legítimo das empresas na coleta e processamento de dados dos colaboradores a fim de conduzir suas

atividades econômicas de forma mais eficiente, diante do potencial lesivo de acesso, armazenamento e distribuição de seus dados pessoais, principalmente quanto ao seu uso para a celebração de acordos com a administração pública, de forma a cumprir com o objetivo principal desta pesquisa.

REFERÊNCIAS BIBLIOGRÁFICAS

ACFE. **Report to the Nations, 2020 global study on occupational fraud and abuse**. Disponível em: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf. Acesso em: fevereiro de 2021.

ARTESE, Gustavo. **Compliance digital: proteção de dados pessoais**. In: CARVALHO, André Castro et. al. Manual de Compliance. Rio de Janeiro: Forense, 2019.

ATHAYDE, Amanda. **Manual dos Acordos de Leniência no Brasil:** teoria e prática – CADE, BC, CVM, CGU, AGU, TCU, MP. 1. REIMPR. Belo Horizonte: Fórum, 2019.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 1989, vol. 2.

BERTOCCELLI, Rodrigo de Pinho. **Compliance.** In: CARVALHO, André Castro et. al. Manual de Compliance. Rio de Janeiro: Forense, 2019.

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

BRASIL. **Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: dezembro de 2020.

BRASIL. **Lei no 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente (ECA)**. Brasília, DF: Presidente da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: junho de 2020.

BRASIL. **Lei nº 12.965/2014, de 23 de abril de 2014**. **Marco Civil da Internet**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: dezembro de 2020.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: dezembro de 2020.

BUCAR, Daniel; VIOLA, Mario. **Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos**. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Editora Revista dos Tribunais, 2019.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional**. 8ª ed. São Paulo: Saraiva, 2014.

BLUM, Rita Peixoto Ferreira; MORAES, Helio Ferreira. **Lei Geral de Proteção de Dados Pessoais - LGPD**. *In*: CARVALHO, André Castro *et. al*. **Manual de *Compliance***. 2. ed. Rio de Janeiro: Forense, 2020.

CARVALHO, A. P. G. **O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos**. Revista de Direito do Consumidor. São Paulo, 2003.

CASTELLS, Manuel. **O Poder da Comunicação**. São Paulo: Paz e Terra, 2015.

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

CUEVA, Ricardo Villas Bôas. **Funções e finalidades dos programas de compliance**. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

Deloitte. **Orientações para celebração de acordos de cooperação por empresas**: Pesquisa "Acordos de Cooperação – Percepção do Empresariado sobre o Tema e Práticas Adotadas". IBDEE, agosto de 2018.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. **Curso de Direito Civil: Responsabilidade Civil**. 5. ed. Salvador: Juspodivm, 2018.

FERREIRA, Luiz Alexandre Cruz. **O direito de defesa na concepção dos atos administrativos. Revista jurídica, [s.l.], 2012**. Disponível em: https://www.uniaraxa.edu.br/ojs/index.php/juridica/article/viewFile/84/76. Acesso em: janeiro de 2021.

FERREIRA FILHO, M. G. **Curso de direito constitucional**. 33ª ed. rev. e atual. São Paulo: Saraiva, 2007.

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

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

GUERRA, Sidney. **O direito à privacidade na internet: uma discussão da esfera privada no mundo globalizado**. Rio de Janeiro: América Jurídica, 2004.

IBGC. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa#:~:text=Governan%C3%A7a%20corporativa%20%C3%A9%20o%20sistema,controle%20e%20demais%20partes%20interessadas. Acesso em: janeiro de 2021.

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

LAMBERTY, Andrey. ISAIA, Cristiano. SILVA, Rosane. **Os desafios do processo e da jurisdição no Estado democrático de direito: elementos de uma teoria da decidibilidade adequada à proteção de dados pessoais do trabalhador.** Revista Eletrônica de Direito Processual – REDP, Rio de Janeiro. Ano 14. Volume 21. Número 3. Setembro a Dezembro de 2020.

LEONARDI, Marcel**. Legítimo interesse**. Revista do Advogado, v. 39, 2019.

LORENZ, Moritz. ***An introduction to EU competition law***. Cambridge University Press, 2013.

MATEUCCI, C. R. F. **Privacidade e internet**. Revista de Direito Privado, São Paulo, ano 5, p.46-55, jul.-set. 2004.

MATTOS FILHO, VEIGA FILHO, MARREY JR. E QUIROGA ADVOGADOS. **Guia para a Lei Geral de Proteção de Dados**. São Paulo. 2018. Disponível em: https://publicacoes.mattosfilho.com.br/books/bdtv/#p=1. Acesso em: janeiro de 2021.

MENDES, Francisco Schertel. **Compliance: concorrência e combate à corrupção**. São Paulo: Trevisan Editora. 2017.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 12. ed. São Paulo: Saraiva, 2017.

MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil**. Revista de Direito do Consumidor, Brasília, v. 120/2018, p. 471, nov./dez. 2018ª.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 2a ed. Curitiba: Juruá Editora, 2004.

PEREIRA DE SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. **Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais**. Direito Público, v. 16, n. 90, dez. 2019.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 LGPD**. São Paulo: Saraiva Educação, 2018.

RIBEIRO, Márcio de Aguiar. **Responsabilização administrativa de pessoas jurídicas à luz da Lei Anticorrupção Empresarial**. Belo Horizonte: Fórum. 2017.

ROCHA, Camila P D et al. **Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD**. Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, v. 2, n. 3, p. 78-97, 2019.

RODOTÁ, Stéfano. **A vida na sociedade de vigilância – a privacidade hoje**. São Paulo: Renovar, 2008.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 7. ed. São Paulo: Saraiva, 2018.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014.

SILVA, De Plácido e. **Vocabulário jurídico**. 28. ed. Rio de Janeiro: Forense, 2009.

SILVA, J. A. **Curso de direito constitucional positivo**. 29.ed. São Paulo: Malheiros, 2007. p. 206.

TJRJ, **26ª Câmara Cível, Apelação Cível nº 0393241-25.2015.8.19.0001**, Relatora Natacha Nascimento Gomes Tostes Gonçalves de Oliveira, j. 22/11/2018, DJ: 22/11/2018.

TJRS. **18ª Câmara Cível, Apelação Cível nº 70069154854**, Relator Túlio de Oliveira Martins, j. 30/06/2016, DJE: 08/07/2016.

TJSP, **33ª Câmara de Direito Privado, Apelação Cível 4007792-98.2013.8.26.0577**, Relator: Mario A. Silveira, j. 30/11/2015, DJE 01/12/2015.

VIANNA, C. S. M. **Da privacidade como direito fundamental da pessoa humana**. Revista de Direito Privado, São Paulo, ano 5, p.102-115, jan.-mar. 2004.

VIDAL, Gabriel. **Conceituação do direito à privacidade em face das novas tecnologias**.

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harward LR, Harward, v. 4, n. 5, p. 193-220, 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: dezembro de 2020.