UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

GABRIELA VICTÓRIA MIRANDA NUNES

GOVERNANÇA E BOAS PRÁTICAS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: DOS PROGRAMAS DE *COMPLIANCE*

Brasília

2019

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

GOVERNANÇA E BOAS PRÁTICAS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: dos programas de *compliance*

Autora: Gabriela Victória Miranda Nunes

Orientadora: Prof. Dra. Laura Schertel Mendes

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.

03 de dezembro de 2019

FOLHA DE APROVAÇÃO

GABRIELA VICTÓRIA MIRANDA NUNES

Governança e Boas Práticas na Lei Geral de Proteção de Dados Pessoais: dos programas de *compliance*

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.

Aprovada em: 03 de dezembro de 2019

BANCA EXAMINADORA

Prof. Dra. Laura Schertel Mendes

(Orientadora – Presidente)

Prof. Dr. Alexandre Veronese

(Membro)

Prof. Me. Fernanda Lage

(Membro)

NUNES, Gabriela Victória Miranda

NN972g **Governança e Boas Práticas na Lei Geral de Proteção de Dados Pessoais: dos programas de *compliance*/** Gabriela Victória Miranda Nunes; orientadora Laura Schertel Mendes -- Brasília, 2019.

67 p.

Monografia (Graduação – Direito) – Universidade de Brasília, 2019.

1. Lei Geral De Proteção De Dados – Contexto Internacional, Conceitos e Principais Normas. 2. Das Boas Práticas e Governança Empresarial. 3. Compliance à Lei Geral de Proteção de Dados. I. Mendes, Laura Schertel, orient. II. Título.

AGRADECIMENTOS

Reservo esse momento para agradecer principalmente a minha mãe, minha melhor amiga e companheira, dona Cristiane, obrigada por sempre me apoiar em todas as minhas decisões e ser a minha voz da consciência. Obrigada por todos os ensinamentos, espero um dia poder retribuir, pelo menos um pouco, tudo o que a senhora já fez por mim durantes todos esses anos.

Gostaria de agradecer o meu irmão mais velho Christopher por ser literalmente a minha inspiração, espero ter metade dessa inteligência e força. Obrigada por sempre estar do meu lado e por me ajudar nas principais decisões que eu já tomei na minha vida.

Gostaria de agradecer os meus amigos, desde a infância à faculdade, obrigada por me fazerem enxergar a vida com mais leveza e alegria. Sem vocês eu com certeza seria uma pessoa muito rabugenta e ranzinza.

Por fim, mas não menos importante, gostaria de agradecer a todos os professores que já passaram pela minha vida. Os ensinamentos que aprendi e até mesmo as lições de vida que me foram dadas, são algo que vou levar para sempre. Obrigada pelo o apoio e o incentivo incansáveis, espero poder um dia impactar a vida de outras pessoas assim como os senhores impactaram a minha. Os meus singelos agradecimentos.

A todos muito obrigada!

Gabriela Victória Miranda Nunes

Brasília, 03 de dezembro de 2019.

RESUMO

O presente trabalho analisa as principais mudanças ocorridas com o advento da nova Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), principalmente no âmbito da governança e boas práticas. Em uma sociedade extremamente direcionada para a coleta e uso de dados, a segurança da informação se tornou indispensável nos tempos atuais. Em um momento no qual leis de proteção de dados estão sendo aprovadas no mundo inteiro, a necessidade de adequação por parte tanto do Poder Público como privado aumentaram. O cenário de coleta e tratamento de dados mudou drasticamente. A partir de revisões bibliográficas nacionais e internacionais, analiso as principais práticas sugeridas para a construção de um efetivo programa de *compliance* e a sua efetivação.

Palavras-chave: Lei Geral de Proteção de Dados (Lei nº 13.709/2018), proteção de dados, *Compliance*, Governança.

ABSTRACT

This paper analyzes the main changes occurred with the approval of the new General Data Protection Act (Federal Statute No. 13.709 / 2018), mainly in the field of governance and good practices. In a society that is extremely focused on data collection and its use, data protection is imperative nowadays. At a time when data protection legislations are being approved around the world, the need for adequacy by both public and private authorities has increased. The data processing landscape has changed dramatically. From national and international bibliographic reviews, I analyze the main suggested practices for the construction of an effective *compliance* program and its implementation.

Keywords: Brazilian General Data Protection Act (Federal Statute No. 13.709 / 2018), data protection, *Compliance*, Governance.

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

CF – Constituição Federal

DPO – *Data Protecion Officer*

LGPD – Lei Geral de Proteção de Dados Pessoais

RGPD – Regulamento Geral Sobre Proteção de Dados

SUMÁRIO

INTRODUÇÃO

O uso indevido de dados pessoais por entidades públicas e privadas é reconhecidamente um grande problema na sociedade atual. Constantemente somos bombardeados com informações sobre o mau uso ou a falta de segurança dos nossos dados. Diante deste cenário, a proteção de dados pessoais se tornou tema importante no contexto jurídico internacional, tendo o Regulamento Geral de Proteção de Dados Europeu assumido função de modelo de legislação sobre a proteção de dados, influenciando diversas legislações acerca do tema. Seguindo esta esteira, o Brasil em 2018, passou a fazer parte dos países que contam com uma legislação específica sobre proteção de dados pessoais e privacidade dos seus cidadãos.

A Lei Geral de Proteção de Dados (LGPD - Lei 13.709/2018), entrará em vigor em agosto de 2020, trazendo consigo grandes modificações no cenário brasileiro de proteção de dados. Concebida com aspectos voltados para a proteção do cidadão contra o tratamento indevido de seus dados, a regulamentação brasileira, trouxe grandes inovações ao cenário regulatório que irão afetar diversas áreas de atuação, tanto público como privado. A aplicação da Lei impactará não somente as instituições brasileiras, como também as organizações nacionais ou estrangeiras que ofertam produtos e/ou serviços para aqueles que residem no Brasil. Desta forma, a nova legislação está ensejando mudanças na maneira como as empresas lidam com os dados on-line e off-line dos seus usuários.

Não é de hoje que existem legislações que regulamentam questões relacionadas à privacidade e proteção de dados, legislações anteriores à LGPD, como o Código de Defesa do Consumidor e o Marco Civil da Internet, já tratavam sobre a necessidade de regulação do uso e coleta de dados. Por meio da Lei Geral de Proteção de Dados foram consolidadas em uma única legislação as principais normas referentes ao tratamento de dados pessoais – como definições, bases legais, princípios, direitos do titular e obrigações dos agentes de tratamento – conferindo assim maior segurança e transparência para todo o sistema de processamento de dados. Nesse sentido, pode se falar em um novo paradigma para a proteção de dados.

A Lei surge com o principal intuito de assegurar o direito à privacidade e à proteção de dados pessoais dos cidadãos, por meio de práticas transparentes e seguras, garantindo direitos e liberdades fundamentais. A partir o estabelecimento de um regramento único e padronizado para o tratamento de dados, confere-se maior segurança, não somente para os

titulares de dados, como também para todos os agentes de tratamento, ao estipular regras claras e precisas sobre tratamento de dados pessoais por empresas, além de promover a concorrência no mercado, a livre iniciativa e a defesa dos princípios de proteção ao consumidor.

Todas as empresas que fazem tratamento de dados pessoais deverão tomar uma série de medidas para garantir a sua conformidade com a nova legislação, devendo implementar políticas corporativas adequadas para a utilização de recursos de tecnologia da informação e capacitação de seus funcionários.

As sanções pela não conformidade incluem desde a advertência, multa ou até mesmo o bloqueio ou eliminação total dos dados pessoais a que se refere a infração. As multas podem variar desde 2% do faturamento do ano anterior até R$ 50 milhões. Além da aplicação dessas sanções a ocorrência de problemas relacionados com a segurança ou tratamento de dados podem causar problemas sérios a própria imagem e reputação da empresa. É nesse sentido que a instituição de uma cultura de *compliance* voltada para a proteção de dados dos titulares é medida urgente e necessária por todos os agentes de tratamento, sejam eles operadores ou controladores.

1. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – CONTEXTO INTERNACIONAL, CONCEITOS E PRINCIPAIS NORMAS

Em razão dos recentes escândalos envolvendo a má utilização de dados coletados eletronicamente, as discussões sobre privacidade na era digital voltaram a ser protagonistas de intensos debates no mundo[1]. Surgiu então, a necessidade da criação de uma regulamentação que tratasse de forma efetiva sobre a temática de proteção de dados pessoais. Não somente como uma forma de prevenir que futuras infrações venham a ocorrer, como também, para conferir maior credibilidade e confiança para esse novo sistema econômico que está crescendo a níveis nunca imaginados.

Sancionada em agosto de 2018, a Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece diretrizes e sanções para o uso e tratamento de dados pessoais. Caracterizada pelo seu objetivo de proteger o cidadão contra os riscos do tratamento de dados, a lei trará grandes modificações no cenário brasileiro de proteção de dados pessoais, se adequando assim aos parâmetros estabelecidos mundialmente. O Brasil com a publicação da LGPD, se nivelou a diversos modelos internacionais com um alto padrão de proteção de dados pessoais.

Criada para estabelecer regras mais claras e precisas ao tratamento de dados pessoais, a LGPD tem como principal intuito gerar maior *accountability* e transparência para os agentes de tratamento de dados, seja esta pessoa natural ou pessoa jurídica, de direito público ou privado. Assegurando assim, por meio de práticas transparentes e seguras, o direito à privacidade e a proteção de dados pessoais dos cidadãos, garantindo direitos e liberdades fundamentais. A LGPD está alicerçada em cinco eixos principais sendo eles: "i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes."[2]

---

[1] O caso mais comum a ser mencionado está relacionado às infrações cometidas pela empresa Cambridge Analytica, a qual é acusada de manipular os dados pessoais de mais de 50 milhões de usuários da rede social Facebook. Baseando-se em dados coletados do aplicativo móvel, a empresa conseguiu realizar um verdadeiro estudo comportamental de seus usuários, chegando a prever suas possíveis ações e tomadas de decisões, acarretando na interferência das eleições de 2016 dos EUA e no Brexit. Para maiores informações acessar o relato investigativo feito pelo The Guardian, no link: https://www.theguardian.com/news/series/cambridge-analytica-files

[2] DONEDA, Danilo; MENDES, Laura Schertel. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, São Paulo, v. 120, p. 469- 483, nov.-dez. 2018.

1.1 Contexto mundial

Não é de hoje que a informação possui poder central em nossa economia. Desde a sociedade industrial até os tempos atuais, o valor auferido ao processo e transmissão de informações vem aumentando a níveis antes inimagináveis. Em decorrência dos grandes avanços tecnológicos ocorridos nas últimas décadas, a nossa economia atual é extremamente voltada para a coleta de informações. Em consequência disso, surgiu uma nova economia de informação e do conhecimento, na qual a Internet adquire papel principal[3]. Para Bioni estamos vivendo em uma verdadeira *sociedade da informação*[4].

A criação de bancos de dados eletrônicos somente evidencia esta nova economia informacional que possui como principal intuito modificar e adequar o comportamento humano as necessidades do mercado.[5]

A grande problemática, além da insegurança com os dados fornecidos e utilizados por determinadas empresas, está direcionada nas camadas mais vulneráveis da população que acabam por serem as mais suscetíveis a possíveis táticas de manipulação, além da possibilidade da utilização dos dados coletados para tomadas de decisões e práticas discriminatórias. A preocupação maior não está somente no uso indevido desses dados coletados, mas nas demais problemáticas que tais atitudes podem acarretar. Um exemplo disso seria o caso já comentado da Cambridge Analytica, que rapidamente, passou de uma discussão relacionada somente a privacidade de dados e ascendeu para discussões sobre a ingerência de empresas particulares em processos democráticos de diversos países. Põem-se

[3] BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento, 2019, p.7. (Versão Minha Biblioteca)

[4] Para o autor a importância dada para o processamento e transmissão de informações na sociedade atual, fez com que houvesse uma reorganização social, no qual "a informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial." A informação é transformada em conhecimento e a partir desse conhecimento se extrai a sua utilidade. "A informação deve ser, assim, convertida em um conhecimento, a fim de torná-la produtiva e estratégica para a atividade empresarial. Por isso, é a matéria-prima de uma economia redimensionada pelos avanços das TICs, destacando-se os dados pessoais dos cidadãos que passam a ditar uma (nova) lógica de acumulação de capital para a geração de riquezas." (____, op. cit. p. 02 e seguintes).

[5] Para a autora Shoshana Zuboff cada momento, decisão, atitude é milimetricamente observado e analisado, o titular de dados passou a ser o próprio produto em pesquisa. Tanto que cada vez mais tem-se conferido maior importância, pelo mercado, a mecanismos capazes de influenciar e modificar opiniões individuais. Estamos vivendo não somente em um capitalismo de vigilância, mas também em uma sociedade de vigilância, no qual "big data" é ao mesmo tempo uma condição e uma expressão. (ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, v. 30, n. 1, p. 75-89, 2015.)

em debate a própria individualidade e autodeterminação humana, visto que, opiniões, crenças e gostos, são sistematicamente manipulados e influenciados, por agentes particulares.

Sistemas cada vez mais complexos capazes de, a partir de uma sofisticada capacidade de processamento, realizar decisões, mapeamentos, estão se tornando progressivamente mais comuns, todavia, a sua forma de funcionamento e gerenciamento ainda são muito obscuros para grande parte da população, muitas das vezes, sem qualquer tipo de transparência ou *accountability*. Impedindo-se assim que haja um controle mais efetivo por parte do usuário sobre a utilização de seus dados. [6]

A facilidade com que esses dados são rastreados acaba por confundir a própria noção de privacidade, criando relações de poder não transparentes e assimétricas entre os analisadores e os analisados, tanto em contextos políticos, como sociais e econômicos[7].

Em razão dessa evidente assimetria e vulnerabilidade do titular de dados foi necessário conferir um tratamento diferenciado daquele concedido na legislação habitual. Como bem delimita Laura Schertel Mendes sobre a questão da proteção de dados:

> "A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados per se, mas a pessoa que é titular desses dados."[8]

Diante deste cenário, aumentou a necessidade de se instituir uma regulação que abarcasse padrões mínimos para o uso e tratamento de dados pessoais. Não somente para proteger o titular contra possíveis ingerências, como também dar maior segurança e estabilidade a este mercado que surge a partir da utilização massiva de dados pessoais. Fortalecendo-se assim a segurança das relações jurídicas e a confiança do titular no tratamento de seus dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.

---

[6] BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento, 2019. (Versão Minha Biblioteca)

[7] GANGADHARAN, Seeta Peña. Digital inclusion and data profiling. Disponível em: http://firstmonday.org/ojs/index.php/fm/article/view/3821/3199. Acesso em: 30/09/2019. Acesso em: setembro de 2019.

[8] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Editora Saraiva, 2014. P. 27

Regular o uso e o tratamento de dados pessoais não somente é necessário como fundamental no cenário atual. Em face dessas novas exigências impostas pelo próprio mercado, foi necessária uma adequação aos parâmetros que estão sendo exigidos mundialmente no tocante a proteção de dados. Dos mais recentes projetos de lei nos EUA, as demais iniciativas regulatórias, diversos países têm intensificado seus esforços para produzir regulamentos sobre proteção de dados pessoais.[9]

Em uma tentativa de fornecer maior segurança para seus cidadãos a União Europeia instituiu um novo regulamento sobre a proteção de dados pessoais, o chamado RGPD (Regulamento Geral Sobre a Proteção de Dados – Regulamento 2916/679) que entrou em vigor no final de maio de 2018.

A Lei Geral de Proteção de Dados (LGPD), tendo como base o próprio RGPD, se torna um dos primeiros regulamentos a se adequar aos novos parâmetros estabelecidos internacionalmente sobre proteção de dados, tornando o Brasil o maior país do mundo, em termos populacionais, que conta com uma lei geral de proteção de dados pessoais[10].

1.2 Proteção de Dados Pessoais como Direito Fundamental

O direito à proteção de dados pessoais está intrinsecamente atrelado ao direito à privacidade. No entanto, reduzir o seu significado somente a este ramo do direito, não englobaria de forma completa toda a sua complexidade. É inegável a relação próxima que o direito à proteção de dados tem com o direito à privacidade, contudo enquanto que este se caracteriza, principalmente pela dicotomia entre as esferas pública e privada, o direito à proteção abarca uma gama de proteção ainda maior[11]. Já que não somente se caracteriza por um direito negativo, de não sofrer interferência alheia, mas sim de um direito de liberdade positiva, no qual o titular tem controle sobre os seus dados, abarcando assim uma gama de proteção mais extensa que aquela conferida ao direito à privacidade.[12]

---

[9] ABRUSIO, Juliana. Com certo atraso, Brasil finalmente é inserido no rol de países com marco legal em proteção de dados. Disponível em: https://www.migalhas.com.br/dePeso/16,MI286385,61044-Com+certo+atraso+Brasil+finalmente+e+inserido+no+rol+de+paises+com . Acesso em: novembro de 2019.

[10] Informação fornecida por Giovanni Butarelli, Supervisor de Proteção de Dados da União Europeia, em seu discurso na 40º Edição da Conferência Internacional de Comissários de Proteção e Privacidade de Dados. Disponível em: https://edps.europa.eu/sites/edp/files/publication/18-10-24_choose_humanity_speech_en_1.pdf . Acesso em: setembro de 2019

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

[12] Ibidem.

Desde que a informação obtida esteja atrelada a uma pessoa identificável, aplica-se o direito à proteção de dados pessoais, mesmo que não tenha relação com a esfera íntima daquela pessoa. É possível perceber esta abrangência no art. 2º da LGPD[13], o qual trata não somente de assuntos relacionados a privacidade do titular dos dados, mas também a demais aspectos que afetam diretamente a vida do titular, abrangendo a sua própria personalidade como um todo.

Neste contexto, percebeu-se, de acordo com Bioni[14], que a única forma eficaz de abarcar a questão da proteção de dados pessoais, seria por meio de sua alocação como uma nova espécie do rol dos direitos da personalidade. Em decorrência de sua extrema complexidade, o direito a proteção de dados necessita de uma regulação própria, que se adeque às suas necessidades e demandas, no qual possa conferir maior segurança e liberdade de autodeterminação ao titular de dados[15], Bioni complementa sua fala ao mencionar que:

> "A sociedade da informação imprime uma nova dinâmica e novos desafios para a proteção da pessoa humana, a começar pela monetização dos seus dados pessoais. Tais dados, além de consolidar uma nova forma de prolongamento da pessoa, passam a interferir em sua própria esfera relacional, reclamando, por isso, uma normatização específica que justifica dogmaticamente a autonomia do direito à proteção dos dados pessoais e os desdobramentos da sua tutela jurídica (e.g., direito de acesso e retificação dos dados e oposição a decisões automatizadas, em especial de práticas discriminatórias)."[16]

Diante desta linha de raciocínio, na própria evolução de um conceito de proteção de dados ligado a privacidade, é importante mencionar uma importante referência sobre o tema que foi a decisão do Tribunal Constitucional alemão no julgamento da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" de 1982[17]. Este julgamento se transformou em um marco histórico sobre o tema, ao reconhecer um direito subjetivo fundamental à autodeterminação informacional, tendo o indivíduo como agente principal. Este julgamento serviu não somente como embasamento para a teoria da proteção de dados,

---

[13] 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.

[14] BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. Gen, Editora Forense, 2019.

[15] Ibidem.

[16] Idem.

[17] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006, p. 193.

como também para a criação de normas nacionais e internacionais sobre o tema[18]. Laura Schertel Mendes complementa afirmando que:

> "[...] a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação." [19]

No ordenamento jurídico brasileiro, a proteção de dados pessoais não é prevista diretamente na Constituição Federal, no entanto, tem-se o entendimento de que este direito pode ser extraído a partir de uma análise dos direitos fundamentais previstos no art. 5º, inciso X (que garantem a inviolabilidade da intimidade e da vida privada), associado com a garantia do *habeas data* e com o princípio fundamental da dignidade humana.[20] Assim entende-se que o direito fundamental à proteção de dados pessoais pode ser visto como uma dimensão da inviolabilidade da intimidade e da vida privada, nos termos da Constituição.[21]

Entretanto, como já debatido anteriormente, vincular a proteção de dados ao direito à privacidade pode limitar a sua atuação.[22] Diante desta obscuridade em nosso ordenamento e em decorrência da sua importância no próprio desenvolvimento como indivíduo, o direito à proteção de dados, já está em fase de ser implementado de forma expressa em nossa Constituição Federal. Aprovado em dois turnos a Proposta de Emenda à Constituição (PEC 17/19), inclui a proteção de dados pessoais, disponíveis em meios digitais, na lista das garantias individuais da CF/88. De relatoria da senadora Simone Tebet no Senado Federal, a proposta tem como principal objetivo resguardar a inviolabilidade das informações dos cidadãos que circulam na internet.[23]

De acordo com a referida Senadora, constitucionalizar a questão de proteção de dados, demonstra o compromisso do país para com o tema. Ela afirma que o Brasil já possui

---

[18] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Editora Saraiva, 2014.
[19] Ibidem.
[20] Idem.
[21] Idem.
[22] "Vê-se, assim, que, embora as garantias de sigilo e de inviolabilidade da intimidade e da privada configurem importantes mecanismos de proteção individual, eles se mostram insuficientes para lidar com os atuais efeitos do processamento e utilização da informação sobre o indivíduo. Afinal, essas garantias visam à proteção específica em face de riscos determinados (divulgação de informações íntimas ou interceptação da comunicação, por exemplo) e não abarcam a totalidade dos riscos aos quais o indivíduo está submetido na sociedade da informação". P. 165.
[23] Para maiores informações acessar o site: https://www12.senado.leg.br/noticias/materias/2019/07/02/protecao-de-dados-pessoais-devera-entrar-na-constituicao-como-direito-fundamental . Acesso em: setembro de 2019

normas infraconstitucionais - a exemplo do Marco Civil da Internet (Lei 12.965, de 2014), da sua regulamentação (Decreto 8.771, de 2016) e da Lei Geral de Proteção de Dados (Lei 13.709, de 2018), no entanto é preciso dar um passo maior e constitucionalizar o tema.[24]

A questão da proteção de dados, como já relatado, vai além da proteção à privacidade, atingindo aspectos da liberdade e da própria identidade pessoal. Desta forma, torna-se necessário um escopo de atuação maior do que aquele fornecido constitucionalmente, a partir da aprovação desta PEC o direito brasileiro preenche essa lacuna e confere uma proteção mais abrangente a questão do tratamento e utilização de dados pessoais.

1.3 Dos Conceitos e Definições

Após uma análise sobre o contexto mundial em que nasceu a Lei Geral de Proteção de Dados, é necessário delimitar os principais conceitos abordados pela lei. É importante ao analisarmos a lei estabelecer primeiramente que por ser uma Lei Geral ela apresenta conceitos amplos e gerais, tendo a LGPD como característica ser abrangente e até por vezes genérica. Diante deste cenário será de responsabilidade da ANPD ser a autoridade responsável pelo estabelecimento e criação de normas mais especificas que se adequem aos diversos ramos empresariais presentes em nossa sociedade.[25]

Antes de prosseguirmos em nossa análise sobre a LGPD é preciso destacar que dados e informação possuem conceitos diversos, apesar de serem tratados como sinônimos na bibliografia atual e na nossa LGPD. Enquanto que dados se referem a fatos brutos ou não processados, a informação é o tratamento desses dados, a fim de se compreender o seu resultado.[26]

> "**Dados** são compostos por fatos básicos, como o nome e a quantidade de horas trabalhadas em uma semana de um funcionário, número de peças em estoque ou pedidos. (...) Quando esses fatos são organizados ou arranjados de maneira significativa, eles se transformam em informações. **Informação** é um conjunto de fatos organizados de modo a terem valor adicional, além de valor propriamente ditos"[27].

[24] Ibidem.
[25] DONEDA, Danilo; MENDES, Laura Schertel.Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, São Paulo, v. 120, p. 469- 483, nov.-dez. 2018.
[26] STAIR, Ralph; REYNOLDS, George W. Princípios de sistema de informação: uma abordagem gerencial. Tradução Flávio Soares Correa. São Paulo: Cengage Learning, 2009.
[27] Ibidem.

Passada essa primeira explicação, poderemos continuar com nossa análise da LGPD.

Em seu art. 5º, a LGPD fornece os principais conceitos e definições na seara de proteção de dados. Primeiramente irei abordar o conceito fornecido aos dados pessoais, que está presente no inciso I, do art. 5º, e é delimitado como qualquer "informação relacionada a pessoa natural identificada ou identificável". Sendo considerado dados sensíveis todos aqueles capazes de revelar "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" (art. 5º, II). [28] É possível perceber a grande semelhança de conceitos, entre a LGPD com o RGPD, já que para a regulação europeia, dados pessoais consistem em[29]:

> Artigo 4º Definições
> Para efeitos do presente regulamento, entende-se por:
> 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;

Importante frisar que assim como no regulamento europeu, o titular dos dados é a pessoa natural a quem os referidos dados são objeto de tratamento (art. 5, V), sendo assim a proteção conferida pela lei não se aplica as pessoas jurídicas, estando elas fora de seu escopo de tutela[30]. Ambos são conceitos centrais da LGPD, que busca proteger a privacidade dos titulares de dados pessoais que sejam objeto de tratamento, considera o dado pessoal uma extensão da personalidade do indivíduo, tendo grande potencial de ferir direitos fundamentais, a lei concedeu um amplo conceito do que se considera como dados pessoais;

---

[28] "A grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo ex ante de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processo eletrônico e ubíquo de dados na sociedade da informação." (DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13,709/2018): o novo paradigma da Proteção de Dados no Brasil. Revista do Consumidor, São Paulo. 2018. P, 22)

[29] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento europeu e Conselho, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 02/10/2019

[30] FRAZÃO, Ana. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial, Parte I. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018 . Acesso em: setembro de 2019

necessidade de se ter uma base legal para o tratamento de dados e tem-se o legitimo interesse como hipótese autorizativa.[31]

Posteriormente, é definido outro importante conceito que é o tratamento de dados, caracterizado por sua amplitude conceitual, ao compreender operações de tratamento de dados realizadas tanto pelo setor público como privado[32]. Além de não possuir restrição de territorialidade, já que a lei tem aplicabilidade extraterritorial, de forma que toda empresa que tratar dados de cidadãos brasileiros ou de estrangeiros que residem no Brasil, mesmo não tendo sede ou filial no Brasil, tem que se regularizar conforme a lei brasileira[33]. O tratamento de dados foi definido pelo inciso X, do art. 5º como:

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

Em decorrência amplitude conceitual de dado pessoal, todo tipo de tratamento de dados pessoais, de forma geral, está submetido a LGPD. Sendo as hipóteses de exceção previstas no art. 4º.[34] É importante destacar que toda operação de tratamento de dados deve estar amparada em uma base legal previstas no art. 7º, destacam-se entre eles, o consentimento, a execução de um contrato, o dever legal do controlador, o tratamento pela administração pública e o legitimo interesse, entre outros. Em relação ao legitimo interesse, este comporta qualquer interesse protegido pela ordem jurídica, no entanto, é importante frisar que o interesse legítimo não pode sobrepor os direitos do titular, deverá haver uma balanceamento entre os dois, caso isso não ocorra, o tratamento não poderá operar com suporte nessa base legal.[35]

Esse tratamento deverá ser feito pelos agentes de tratamento definidos como: o **controlador**, descrito como toda "pessoa natural ou jurídica, de direito público ou privado,

---

[31] DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados. Op. Cit., p.22
[32] FRAZÃO, Ana, Op. cit.
[33] Art. 3º da LGPD
[34] "I- realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II- realizado para fins exclusivamente jornalístico e artísticos, ou acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III- realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais e IV- provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. "
[35] DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados. Op. Cit., p.23

a quem competem as decisões referentes ao tratamento de dados pessoais" (art.5, VI), o **operador**, descrito como toda "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5, VII) e o **encarregado** que é toda "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (art. 5º, VIII). Essas definições serão de extrema importância para posterior definição de responsabilização de cada agente, a depender de sua função no tratamento e armazenamento de dados.

Em relação a responsabilidade a LGPD adotou o regime de responsabilidade objetiva (art. 42º), no qual vincula-se "a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais."[36]

As demais definições presentes no art. 5º da lei, apesar de sua importância no campo de proteção de dados, não serão analisadas neste momento, por questões de didática e enquadramento no escopo do trabalho.

1.4 Princípios

Como forma a nortear o tratamento de dados e estabelecer orientações quanto aos cuidados e regras que devem ser seguidos na utilização e tratamento de dados, o art. 6º da LGPD estabelece um conjunto de princípios que devem ser adotados, além da observância à boa-fé. Com a proposta de apresentar a melhor dinâmica, irei sistematizá-los em três grupos principais de equivalência.

1.4.1 Da finalidade, adequação e necessidade

Primeiramente irei abordar aqueles que são os princípios norteadores do tratamento de dados. De acordo com estes princípios, os dados coletados devem ter finalidades determinadas e específicas, devendo estar adstrita ao mínimo necessário para a realização de suas finalidades e compatíveis ao contexto transmitido ao titular na coleta de seus dados. Estão descritos pela lei como: o **princípio da finalidade** que é definido como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem

[36] DONEDA, Danilo; MENDES, Laura Schertel. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, São Paulo, v. 120, p. 469- 483, nov.-dez. 2018. P. 5

possibilidade de tratamento posterior de forma incompatível com essas finalidades" (art. 6º, I); **princípio da adequação** descrito como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (art. 6º, II); o **princípio da necessidade** definido como a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados"(art. 6º, III).

É interessante analisar essa gama de princípios pois eles são fundamentais para assegurar que a vinculação do tratamento de dados pessoais à finalidade que motivou e justificou a sua coleta. Assim se traz uma maior segurança para a coleta e tratamento, além de maior transparência para todo o processo.

1.4.2 Do livre acesso, da qualidade de dados e transparência

Estes princípios estão previstos nos seguintes incisos: O **princípio do livre acesso** descrito como a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (art. 6º, IV); o **princípio da qualidade dos dados** descrito como a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (art. 6º, V); o **princípio da transparência** seria a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" (art. 6º, VI).

Esses princípios analisados nada mais são que a consagração da necessidade de utilização de uma linguagem e procedimentos transparentes. O responsável pelo tratamento deve adotar medidas adequadas para fornecer ao titular todas as informações necessárias para o devido cumprimento dos direitos do titular. Além de a comunicação ser de forma clara, simples, coesa e de fácil acesso, possibilitando que o cidadão comum consiga entender as informações que lhe estão sendo prestadas, respeitando os segredos comercial e industrial.

1.4.3 Da segurança, da não discriminação, da responsabilização e da prestação de contas

Por fim, os últimos princípios tratam sobre questões relacionadas à segurança no tratamento dos dados e na sua utilização, vedando práticas discriminatórias, que possam interferir de forma negativa na esfera pessoal do titular, além de prever mecanismo de *accountability* para os agentes de tratamento de dados. Estão previstos nos seguintes incisos: o **princípio da segurança** descrito como a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (art. 6º, VII); o **princípio da prevenção** definido como a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais"(art. 6º, VIII); o **princípio da não discriminação** descrito como "a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos"(art. 6º, IX) e por fim os **princípios responsabilização e prestação de contas** definidos como a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"(art. 6º, X).

A partir dessa análise pormenorizada dos princípios elencados, iremos agora analisar os direitos conferidos aos titulares de dados pela Lei Geral de Proteção de Dados.

1.5 Dos Direitos dos titulares dos dados pessoais

Em seu Capítulo III, a LGPD elenca os principais direitos dos titulares de dados pessoais. É importante destacar que diversos outros direitos e garantias já foram tratados em capítulos anteriores da norma legal, sendo necessário assim, uma análise sistemática e conjunta de toda a legislação, para se desprender o seu real entendimento e extensão.

Isto posto, a descrição dada pelo art. 17, o qual prevê que "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei", é somente exemplificativa

e deve ser analisada em conjunto com os demais artigos da Lei, principalmente aqueles previstos nos arts. 1º e 2º.[37]

Um bom exemplo disso ocorre no artigo seguinte, ao delimitar os direitos do titular dos dados pessoais. O art. 18º afirma que o titular dos dados pessoais tem direito a obter do controlador, de forma gratuita (§5º), em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

> " I - a 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."

É possível perceber que os direitos ali assegurados, com exceção do direito à portabilidade, já foram mencionados anteriormente no escopo da Lei. Desta forma, é imprescindível compreender, como já aludido, que os direitos transcritos nos art. 17 e 18, são meramente exemplificativos e é necessária uma interpretação conjunta de toda o ordenamento, principalmente dos Capítulos I e II, para se ter um entendimento integral da lei. Ultrapassada esta primeira explicação, irei utilizar a tabela elaborada por Ana Frazão em seu artigo intitulado "Nova LGPD: direitos dos titulares de dados pessoais", publicada no JOTA[38], que realiza uma breve sistematização dos direitos conferidos aos titulares de dados, delimitando de forma simples e clara os seus principais contornos.

Direitos específicos dos titulares de dados pessoais	Referência Legislativa
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais.	Arts. 7º, I, e 8º

[37] **Art. 1º** Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
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.

[38] Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-os-direitos-dos-titulares-de-dados-pessoais-17102018. Acesso em: setembro de 2019

Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei mesmo para os casos de dispensa de exigência de consentimento.	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento.	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais.	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.	Art. 9º, § 1º
Direito de revogar o consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado.	Art. 8º, § 5º
Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados	Arts. 8º, § 6º e 9º, § 2º
Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras, finalidade específica do tratamento, forma e duração do tratamento, observados os segredos comercial e industrial, identificação do controlador, informações de contato do controlador, informações acerca do uso compartilhado de dados pelo controlador e a finalidade, responsabilidades dos agentes que realizarão o tratamento, e direitos do titular, com menção explícita aos direitos contidos no art. 18	Art. 9º
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações	Art. 8º, § 6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos	Art. 9º, § 3º
Direito de ser informado sobre a utilização dos dados pela administração pública, para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa	Art. 7º, III e IV c/c art. 7º, § 1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização	Art. 7º, § 3º
Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento	Art. 7º, § 5º
Direito à transparência do tratamento de dados baseado no legítimo	Art. 10, § 2º

interesse do controlador	
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa	Art. 11, II, c
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para tratamento de dados sensíveis nas hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos	Art. 11, § 2º
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular	Art. 11, § 4º
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas	Art. 13
Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública	Art. 13, § 1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa	Art. 13, § 2º
Direito ao término do tratamento quando verificado que (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento, (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou (i) por determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, autorizada a conservação somente nas exceções legais	Art. 16

Adiante irei tratar sobre os demais artigos presentes no Capítulo III da LGPD que finaliza a questão dos direitos consagrados aos titulares de dados pessoais.

1.5.1 Da confirmação da existência de tratamento e do acesso aos dados

Complementando o que foi disposto no Capítulo II, o art. 19 trata sobre o direito de acesso aos dados pelo titular, conforme o dispositivo:

> "A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular."

É possível perceber a aplicação dos princípios da transparência, do livre acesso e da qualidade de dados, ao assegurar ao titular o livre acesso ou a confirmação de existência de dados pessoais que estejam sob os cuidados de agentes de tratamento. Devendo esta informação ser repassada de forma simplificada e no prazo máximo de 15 dias para casos mais complexas. Importante destacar que, de acordo com o §4 "A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos."

Posteriormente, o §1º e §2º do art. 19 embasam este entendimento ao determina que "Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso", e que "As informações e os dados poderão ser fornecidos, a critério do titular: I - por meio eletrônico, seguro e idôneo para esse fim; ou II - sob forma impressa."

A LGPD buscou garantir a maior celeridade e auxílio possível ao titular de dados, ao assegurar no §3º, em caso específico do tratamento decorrente de consentimento do titular ou em contrato a possibilidade do titular poder "solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento." Delimitando no art. 37, para que este direito possa ser exercido em sua totalidade que "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."

Por fim, nos últimos artigos do Capítulo, trata-se sobre, a possibilidade conferida aos titulares a correção de eventuais erros, inexatidões ou desatualizações que possam lhes gerar

prejuízos[39]. Tendo o direito à correção de dados incompletos, inexatos ou desatualizados grande importância em demais direitos, como o direito de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais (LGPD, art. 20), já que abre-se a possibilidade para a readequação dos dados utilizados, como bem relata Ana Frazão.[40]

1.6 Da Autoridade Nacional de Proteção de Dados (ANPD)

Instituída pela Lei nº 13.853, de 8 de julho de 2010 e sancionada pelo presidente Jair Bolsonaro, a Autoridade Nacional de Proteção de Dados (ANPD), criada pela Medida Provisória nº 869/2018. A ANPD será o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Vinculada à Presidência da República, a ANPD possuirá natureza transitória de órgão da administração pública federal, podendo ser transformada em autarquia até o prazo máximo de 2 anos, a critério do Poder Executivo[41]. Tendo a priori, sido assegurado sua autonomia técnica e decisória pela lei, apesar de ser vinculada administrativamente à Presidência[42].

Quanto a sua estrutura interna, a ANPD deverá conter os seguintes órgãos: I. Conselho diretor; II. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III. Corregedoria; IV. Ouvidoria, V. Órgão de assessoramento jurídico próprio; VI. Unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei[43].

Devendo o Conselho Diretor ser composto por 5 membros, que serão escolhidos pelo Presidente da República, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal. O mandato será de 4 anos, somente podendo ser removido em virtude de renúncia, condenação judicial transitada em julgado ou pena de

---

[39] Referente a 9ª parte de uma série sobre as repercussões da LGPD para a atividade empresarial, artigo intitulado "Nova LGPD: direitos dos titulares de dados pessoais" de Ana Frazão. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direitos-dos-titulares-de-dados-pessoais-24102018. Acesso em: 25/08/2019

[40] FRAZÃO, Ana. Op. Cit.

[41] Art. 55-A, §1 da LGPD

[42] A grande preocupação de grandes estudiosos do tema é que, em decorrência de sua vinculação à Presidência da República, além de o órgão não possuir orçamento independente e receber ordens diretas da Presidência, a sua autonomia ficara prejudicada, além de ter possíveis conflitos de interesse, já que a lei aborda diretamente sobre tratamento de dados do próprio setor público. Para maiores informações conferir o artigo de Alexandre Leoratti sobre o tema. Disponível em: https://www.jota.info/legislativo/autoridade-de-protecao-dados-autonomia-30122018 . Acesso em: 30/10/2019

[43] Art. 55-C da LGPD

demissão decorrente de processo administrativo disciplinar. Sendo de atribuição do Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis.

Já o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, será composto de 23 (vinte e três) representantes de órgãos e entidades da administração pública, da sociedade civil, de instituições científicas, de confederações sindicais, do setor empresarial e laboral. Serão designados por ato do Presidente da República, sendo que, excluídos os representantes de órgãos e entidades da administração pública, os demais integrantes, não poderão ser membros do Comitê Gestor da Internet no Brasil e terão mandato de 2 (dois) anos, permitida 1 (uma) recondução.

Dentre as competências da ANPD, destaco o dever de zelar pela proteção dos dados pessoais e pela observância dos segredos comercial e industrial, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, além de promover a conscientização na população acerca da proteção de dados pessoais, bem como a realização de audiências públicas, além de ter o papel central de garantir os direitos dos cidadãos sobre os seus dados.

A ANPD é indispensável para a efetividade da lei. Em decorrência de sua importância, a ANPD é a responsável por garantir que lei esteja sendo de fato cumprida, mantendo padrões persistentes de aplicação da legislação.[44] Sendo ela a autoridade incumbida de estabelecer os parâmetros a serem aplicados, elaborando normas e regulamentos relacionados a proteção de dados, além do dever de proporcionar um equilíbrio entre as atividades desenvolvidas e os padrões estabelecidos, respeitando as características dos diversos setores que fazem tratamento de dados e as peculiaridades de cada empresa. Para que a ANPD possa cumprir o seu papel de forma eficaz é preciso que a autoridade esteja amparada no seguinte tripé: independência, poder sancionatório e expertise.[45]

[44] DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13,709/2018): o novo paradigma da Proteção de Dados no Brasil. Revista do Consumidor, São Paulo, 2018. P. 24-25.
[45] Ibidem.

1.6.1 Das Sanções Administrativas

A Lei visa garantir que todos os seus preceitos sejam cumpridos de forma efetiva, sendo assim para que esta realidade seja possível, o legislador achou por necessário a instituição de duras punições para o seu descumprimento. As sanções administrativas para o descumprimento da LGPD estão previstas no art. 52º da LGPD, sendo de competência exclusiva da ANPD a sua aplicação. São elas:

I. advertência, com indicação de prazo para adoção de medidas corretivas;
II. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III. multa diária, observado o limite total a que se refere o inciso II;
IV. publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI. eliminação dos dados pessoais a que se refere a infração;
VII. suspensão parcial do funcionamento do banco de dados por até seis meses;
VIII. suspensão do tratamento dos dados pessoais a que se refere a infração;
IX. e proibição parcial ou total de exercer atividades de tratamento de dados.

As sanções somente poderão ser aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa. Sendo que o valor aplicável às sanções multa diárias deverá observar a gravidade da falta e a extensão do dano ou prejuízo causado[46].

1.8 Considerações finais

Terminada esta análise introdutória sobre a Lei Geral de Proteção de Dados, delimitando os seus principais aspectos e definições. No próximo capítulo irei abordar sobre o tema central deste presente trabalho que é a questão das boas práticas e da governança, em respeitos as estipulações definidas na Lei 13.709, delimitando quais são as suas principais

[46] art. 54 da LGPD

funções, quais são os principais perigos e desafios para a sua efetividade, e como a mudança de cenário na cultura corporativa é fundamental para que a lei consiga ser de fato efetiva.

2. DAS BOAS PRÁTICAS E GOVERNANÇA EMPRESARIAL

A partir da crescente importância que o tratamento de dados adquiriu em nossa sociedade atual, passando a ser matéria primordial em nossa economia, como discutido anteriormente, as empresas estão cada vez mais abordando a coleta e o tratamento de dados pessoais como recursos indispensáveis para a continuidade e efetividade de seus negócios (economia baseada em dados).[47] A ocorrência de crescentes casos de abusos cometidos contra a privacidade dos cidadãos, por parte do governo e de corporações, fez surgir a necessidade não somente de legislações específicas que regulamentem o uso indevido de dados, como também, fez-se necessária a criação de mecanismos que cumprimento e a adesão por parte das empresas à normas éticas e legais de conformidade.[48]

Vivemos em um momento único de transformação, no qual a sociedade de forma geral não aceita mais atos e práticas abusivas para com os seus dados. O cenário atual está mudando rapidamente, não somente no que concerne ao tratamento de dados, mas também na propagação de uma política de responsabilização por parte do setor privado em todas as áreas, estabelecendo um novo grau de ética empresarial.[49] É possível perceber essa mudança de comportamento corporativo, a partir da adoção por parte de diversos países, de legislações que buscam pela integridade e combate à corrupção, cabendo aqui destacar, o *Foreign Corrupt Practices Act* - FCPA, editado nos Estados Unidos em 1977, a U.S. *Sentencing Guidelines* de 1991, o *UK Bribery Act* - UKBA, e no âmbito brasileiro temos como destaque a Lei Anticorrupção (Lei nº 12.846) e a Lei das Estatais (Lei nº 13.303).[50] Indo nesta mesma direção, o termo *compliance* está se tornando cada vez mais presente em nossa realidade, e a mera adoção a um programa de conformidade, sem que de fato seja comprovado a sua efetividade, não é suficiente para a adequação aos parâmetros que estão sendo estabelecidos mundialmente sobre o tema.[51]

> "Dentro de um contexto de mudanças tecnológicas constantes e aceleradas, com reflexos nas relações político-econômicas e sociais, são necessários o crescimento e a modernização da indústria e da prestação de serviços, com base não apenas na inovação, incorporação de novas tecnologias e capital, mas também na capacidade de gerenciamento das organizações, que devem desenvolver a competição de forma objetiva e em crescentes níveis de qualidade e produtividade." [52]

[47] BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. Gen, Editora Forense, 2019.

Foi dentro deste novo paradigma que nasce a necessidade da instituição não somente de um programa de *compliance* efetivo, como também de uma governança corporativa efetiva. Mecanismo este destinado para a criação de regras de boas práticas e de governança que estabeleçam procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais[53]. É referente a mudança na própria cultura empresarial, sendo caracterizada por uma mudança de "dentro para fora". As corporações passam a assumir papel de protagonismo neste sistema e não somente de observância aos regramentos impostos pelo Poder Público, tendo as práticas de governança assumido papel importante de autorregulação. [54]

2.1 Contexto e amplitude

Antes de tratarmos do *compliance* em si, é importante primeiramente abordar a questão geral da boa governança, sendo de importantíssimo valor a contextualização da governança corporativa, como mecanismo em que se enquadra a instituição e adoção de programas de *compliance*.

A governança corporativa se relaciona diretamente com as práticas do alto escalão de uma empresa, incluindo seu conselho administrativo, acionistas e demais interessados.[55] Se caracteriza por ser uma relação estritamente horizontal em sua origem, em que a alta direção é responsável direta pela composição de ações estratégicas para supervisionar o desenvolvimento do negócio, e que posteriormente adquire características verticais, sendo o sistema pelo qual as companhias são dirigidas e controladas.[56] De acordo com o Instituto

[48] Ibidem.
[49] OLIVIA, Milena Donato; SILVA, Rodrigo da Guia. Origem e evolução histórica do *compliance* no direito brasileiro. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.
[50] Ibidem.
[51] SILVA, Edson Cordeiro da. *Ġovernança corporativa nas empresas*. 4. ed. atual. rev. São Paulo: Atlas, 2016. p, 6. (Versão digital)
[52] Ibidem.
[53] Ibidem.
[54] Idem.
[55] ALMEIDA, Luiz Eduardo de. Governança Corporativa. In: VENTURINI, Otavio Venturini et al (Coord.). Manual de *Compliance*. Rio de Janeiro: Forense, 2019. p, 13. (Versão Minha Biblioteca)
[56] Ibidem.

Brasileiro de Governança Corporativa - IBGC, em seu Código de Melhores Práticas, a governança é tida como um sistema de relações no qual[57]:

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

Existem diversas definições de governança corporativa, mas de forma geral a essência teórica permanece a mesma. A governança corporativa parte de um contexto econômico e político bastante abrangente, no qual, a partir da atuação de diversos agentes, busca-se primordialmente incentivar e manter as condições de boas práticas, possibilitando assim que as empresas cumpram o seu papel social[58]. Para a OCDE (Organização para a Cooperação e Desenvolvimento Econômico), a governança é tida como guardiã de direitos:

> "A governança corporativa é o sistema segundo o qual as corporações de negócio são dirigidas e controladas. A estrutura da governança corporativa especifica a distribuição dos direitos e responsabilidade entre os diferentes participantes da corporação, tais como o conselho de administração, os diretores executivos, os acionistas e outros interessados, além de definir as regras e procedimentos para a tomada de decisão em relação às questões corporativas. E oferece também bases através das quais os objetivos da empresa são estabelecidos, definindo os meios para se alcançarem tais objetivos e os instrumentos para se acompanhar o desempenho" [59]

Os mecanismos de governança corporativa, para que sejam considerados eficientes, são divididos pela doutrina em internos e externos, tendo como principal objetivo assegurar que a tomada de decisões seja baseada no melhor interesse e que propicie a geração de valor a longo prazo para os acionistas.[60] Edson da Silva complementa afirmando que estes mecanismos são necessários em decorrência de três potenciais problemas que poderiam

---

[57] IBGC (2018). *Código das melhores práticas de governança corporativa*, p. 20. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138 .Acesso em: outubro de 2019.

[58] ALMEIDA, Luiz Eduardo de. Governança Corporativa. In: VENTURINI, Otavio Venturini et al (Coord.). Manual de *Compliance*. Rio de Janeiro: Forense, 2019. p, 13. (Versão Minha Biblioteca)

[59] OCDE - Princípios da Governança Corporativa - 1999. Por fim, importante mencionar a conceituação da governança corporativa como estrutura de poder dada por Cadbury no qual "A governança corporativa é o sistema e a estrutura de poder que regem os mecanismos através dos quais as companhias são dirigidas e controladas" (CADBURY COMMITTEE. The report of the committee on financial aspects of corporate governance. Londres: Cadbury Committee, Dec. 1992.)

[60] SILVA, Edson Cordeiro da. Op.cit.p, 36. (Versão Minha Biblioteca)

interferir na gestão da empresa, seriam eles: vieses cognitivos, conflitos de interesses e limitações técnicas individuais[61]. Estes mecanismos se dividem em[62]:

a) Mecanismos internos: São os responsáveis pela observância dos preceitos legais e éticos que governam a empresa. As boas práticas de governança partem de dentro para fora. Compõem-se pelos órgãos de governança (tais como o conselho de administração, *compliance* e controles internos) e os demais empregados.
b) Mecanismos externos: já nos mecanismos externos as boas práticas partem de fora da organização e são utilizados para auxiliar as empresas a manterem comportamentos éticos e transparentes, além de mediar as relações entre as partes interessadas. Constituem-se pelo sistema legal, auditorias externas, *enforcement*, agências de rating, competição de mercado, entre outros.

61 Ibidem.
62 AGUILERA, Ruth V. et al. Connecting the dots: Bringing external corporate governance into the corporate governance puzzle. **The Academy of Management Annals**, v. 9, n. 1, p. 483-573, 2015.

2.2 Princípios

Como bem relata Andrade e Rosseti[63] os princípios são a base ética da governança e possuem como principal característica a sua universalidade. Por meio destes busca-se "manter e incentivar as condições das boas práticas de governança"[64], colaborando para que a sua função social seja cumprida. Os princípios que regem a governança corporativa, de acordo com o IBGC, podem ser divididos em[65]:

> "Transparência - Consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que conduzem à preservação e à otimização do valor da organização.
>
> Equidade - Caracteriza-se pelo tratamento justo e isonômico de todos os sócios e demais partes interessadas (*stakeholders*), levando em consideração seus direitos, deveres, necessidades, interesses e expectativas.
>
> Prestação de contas (*accountability*) - Os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis.
>
> Responsabilidade Corporativa - Os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional etc.) no curto, médio e longo prazos."

2.3 Dos programas de integridade e de governança

Também chamados de programas de conformidade, de cumprimento ou de integridade, os programas de *compliance* são instrumentos de controle criados para garantir

---

[63] ROSSETTI, José Paschoal; ANDRADE, Adriana. Governança corporativa: fundamentos, desenvolvimento e tendências. 7. ed. São Paulo: Atlas, 2014.

[64] "[...] Buscam criar, manter e incentivar as condições das boas práticas de governança, de modo a que a pessoa jurídica cumpra sua função social colaborando com o desenvolvimento econômico, com a geração de empregos, o desenvolvimento regional, a utilização racional de recursos naturais, e, também, agregando valor e gerando resultados positivos aos associados, sócios ou acionistas (*shareholders*) e oferecendo incentivos adequados a todas as partes interessadas (*stakeholders*)." (ALMEIDA, Luiz Eduardo de. Governança Corporativa. In: VENTURINI, Otavio Venturini et al (Coord.). Manual de *Compliance*. Rio de Janeiro: Forense, 2019. p, 14.)

[65] IBGC (2018). *Código das melhores práticas de governança corporativa*, p. 20-21. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138 Acesso em: outubro de 2019. Importante destacar que o Código considera como agentes de governança os "indivíduos e órgãos envolvidos no sistema de governança, tais como: sócios, administradores, conselheiros fiscais, auditores, conselho de administração, conselho fiscal etc." p.13.

a observância de preceitos legais e éticos.[66] Enfatizando a prevenção de riscos de responsabilidade empresarial pelo descumprimento de normas legais e regulatórias, com o intuito de evitar o cometimento de ilícito.[67] Preza-se pela eficiência na adoção e mudanças do próprio comportamento corporativo, estabelecendo padrões de conduta a serem observados, não somente por funcionários, mas como também pela alta direção, incluindo administradores e demais colaboradores.[68]

> "[...] o *compliance* está fundamentado no conceito de "bom cidadão", consubstanciado na fidelidade à legalidade, na existência de controles internos e externos, na limitação e no equilíbrio de poder, entre outros. Outro aspecto importante é a exigência de comprometimento da alta administração, o que mostra o potencial do *compliance* de reconfigurar o próprio dever de diligência dos administradores, que passa a assumir uma importante dimensão organizacional."[69]

Governança corporativa e *compliance* estão intimamente conectados, sendo complementares entre si. No entanto, é de fundamental importância que estes dois conceitos não sejam confundidos. Enquanto que a governança corporativa está mais comprometida com questões relacionadas a reputação da empresa e as relações entre *stakeholders* internos e externos, prezando pela gestão eficiente e pela transparência, o *compliance*, é responsável pela conformidade com as regras, sendo assim um processo interno. [70] O escopo de atuação de um bom governo vai além de somente cumprir com regras, no entanto, a não existência

---

[66] "Os programas de *compliance*, também chamados de programas de conformidade, de cumprimento ou de integridade, são instrumentos de governança corporativa tendentes a garantir que as políticas públicas sejam implantadas com maior eficiência. Compõem-se de rotinas e práticas concebidas para prevenir riscos de responsabilidade empresarial decorrentes do descumprimento de obrigações legais ou regulatórias. Em complementação às políticas sancionatórias tradicionais, que se fundam na imputação de uma pena correspondente ao ilícito praticado, os programas de *compliance* voltam-se para a mudança de comportamento, por meio de padrões de conduta a serem observados e monitorados pelas empresas, administradores e funcionários, a fim de evitar o cometimento de ilícito." (CUEVA, Ricardo Villas Bôas. Funções e finalidade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p.53-54.)

[67] Ibidem.

[68] Idem.

[69] FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Gurnspun (Coord.) Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2017, p. 43.

[70] Para Domingos Soares Farinho "[...] É fácil confundir-se bom governo com cumprimento de regras (*compliance*), pois existe efetivamente uma ligação estreita entre ambos. Porém , o bom governo de instituições começa antes e acaba depois do cumprimento de regras. Com efeito, o bom governo das empresas estatais implica um conjunto de princípios, regras e procedimentos que visam planear e avaliar o desempenho das empresas públicas para assim se conseguir a máxima eficiência face aos objetivos que lhe são atribuídos. O cumprimento de regras surge como nuclear para garantir o sucesso do planeamento e permitir uma avaliação profícua. [...] A adoção de certos princípios e procedimentos, ainda que não obrigatórios, mas acordados como geradores de maior eficiência, dirá sempre respeito ao cumprimento de regras, mas demonstra que um programa de bom governo só se cumpre com adequada *compliance*, mas está para além dela." (FARINHO, Domingos Soares. Programas de integridade e governança das empresas estatais: uma visão portuguesa no contexto da União Europeia. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 237)

ou falta de estruturação de um programa de cumprimento, pode tornar a governança ineficiente.[71] Desta forma, apesar de serem instrumentos diversos, existe uma correlação entre ambos, atuando separadamente, mas de modo integrado.

2.4 Conceito e alcance dos programas de *compliance*

O termo *compliance* provém da expressão inglesa *"to comply (with)"*, o qual significa cumprir ou agir de acordo com. Tem como principal finalidade garantir que a empresa ou ambiente corporativo, seja de organização pública ou privada, empregue e observe aos princípios que regem as atividades empresariais, de forma que não viole as previsões legais vigentes e procedimentos éticos. [72] Também se refere não somente ao combate ao cometimento de infrações, como também caso já tenha ocorrido o ilícito, auxiliar na condução ao retorno à legalidade e normalidade.[73] De acordo com o Guia – Programas de *Compliance* do Conselho Administrativo de Defesa Econômica (CADE):

> *"Compliance* é um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios ou colaboradores. Por meio dos programas de *compliance*, os agentes reforçam seu compromisso com os valores e objetivos ali explicitados, primordialmente com o cumprimento da legislação. Esse objetivo é bastante ambicioso e por isso mesmo ele requer não apenas a elaboração de uma série de procedimentos, mas também (e principalmente) uma mudança na cultura corporativa. O programa de *compliance* terá resultados positivos quando conseguir incutir nos colaboradores a importância em fazer a coisa certa."[74]

É importante destacar que estar em *compliance* vai além de somente cumprir com as regras formais das empresas, devendo o seu alcance ser mais abrangente, englobando todo o sistema empresarial, servindo como um "instrumento de mitigação de riscos, preservação dos

---

[71] Ibidem.

[72] FRAZÃO, Ana; Medeiros, Ana Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 71.

[73] Ibidem.

[74] *Guia: Programas de Compliance – Conselho Administrativo de Defesa Econômica*, 2016, p. 9. Vale mencionar ainda a definição dada por Ana Frazão "*Compliance* diz respeito ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou , já tendo ocorrido o ilícito, propiciara o imediato retorno ao contexto de normalidade e legalidade." (FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, André Gurnspun (Coord.) Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2017, p. 42)

valores éticos e de sustentabilidade corporativa, preservando a continuidade do negócio e o interesse dos *stakeholders.*"[75]

Tendo como principal propósito à prevenção de infrações e de danos, além do respeito a legalidade, a adoção de programas efetivos de *compliance* traz benefícios que vão muito além de incentivos contidos em lei, abrangendo vantagens em aspectos concorrenciais e atração de consumidores. Sendo o *compliance* de grande importância na proteção e aprimoramento da reputação da empresa. [76]

2.5 Função e conteúdo dos programas de *compliance*

A função primordial dos programas de *compliance* é garantir não somente a obediência à preceitos legais e éticos, mas principalmente, garantir segurança e proteção à empresa, aos administradores e empregados. [77] Oriundo da adoção de mecanismos que prezem pela observância e conformidade, pretende-se assim evitar o cometimento de infrações através de ações organizacionais preventivas.[78] Essa função protetiva dos programas de *compliance*, é fundamental na proteção contra sanções administrativas, civis ou penais que possam de alguma forma danificar a reputação da empresa. [79]

[75] BERTOCCELLI, Rodrigo de Pinho. *Compliance*. In: VENTURINI, Otávio Venturini et al (Coord.). Manual de *Compliance*. Rio de Janeiro: Forense, 2019. p, 37. (Versão digital)

[76] "A adoção do *compliance* é cada vez mais essencial às pessoas jurídicas. Não apenas pelos incentivos legislativos ou por imposição legal, mas também porque o *compliance* atesta a seriedade do agente econômico e, com isso, possibilita mais negócios e maior inserção no mercado. A exigência de programas de integridade não é apenas legislativa, mas dos parceiros comerciais, consumidores, funcionários, porque o *compliance* busca assegurar ambiente corporativo sério, saudável e comprometido com a legalidade. Não por acaso se reconhece que a adoção de programas efetivos de *compliance* pode produzir benefícios para muito além das sanções premiais previstas em lei, podendo gerar expressivas vantagens em aspectos como concorrência, atração dos consumidores e até o incremento do bem-estar dos colaboradores da pessoa jurídica." (OLIVIA, Milena Donato; SILVA, Rodrigo da Guia. Origem e evolução histórica do *compliance* no direito brasileiro. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 48.)

[77] CUEVA, Ricardo Villas Bôas. Funções e finalidade dos programas de *compliance*. IN: Cueva, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 57.

[78] Ibidem.

[79] Idem.

Em conjunção a função protetora do *compliance* é importante destacar também o caráter preventivo que este tem. A conscientização proporcionada por um programa efetivo de *compliance,* no qual ocorre um preparo contínuo de funcionários e administradores, tem como principal consequência a minimização de riscos e uma capacitação maior a identificação de eventuais violações à lei de forma mais rápida e eficiente. [80]

2.6 Da autorregulação

É inegável a importância que a autorregulação possui para a efetividade da regulação estatal sobre a atividade empresarial. Compreende-se que o *enforcement* tradicional, imposto unilateralmente pelo Estado, não é suficiente para garantir que comandos legais sejam de fato cumpridos.[81] Desta forma, os programas de *compliance* servem não somente para delimitar a atuação das empresas de acordo com os preceitos legais, mas serve, principalmente, para a criação de uma ambiente de *compliance,* o qual perpassa todas as camadas de atuação das organizações, seja de parcerias de negócios, a atendimento de consumidores.[82] A participação ativa do setor privado é fundamental para a efetividade das normas legais.

> "Os programas de cumprimento de normas caracterizam-se como modalidade de autorregulação da atividade empresarial, estimulada pelo Estado, cuja capacidade de regular efetiva e tempestivamente a atividade econômica tem se reduzido, em vista da crescente complexidade social, do incessante desenvolvimento tecnológico e da globalização. A chamada autorregulação regulada ou corregulação consiste numa modalidade de regulação que incorpora o ente privado, subordinando-o a fins concretos ou a interesses predeterminados pelo Estado, tal como se dá na disciplina dos programas de *compliance*."[83]

[80] Idem.

[81] "A importância dos programas de *compliance* ganha força em razão das limitações do *enforcement* tradicional, baseado na regulação jurídica estatal e na imposição de sanções. Em uma sociedade cada vez mais complexa, o regime de comando-sanção, unilateralmente imposto e controlado pelo Estado, acaba sendo insuficiente para assegurar a eficácia dos comandos legais." (FRAZÃO, Ana; Medeiros, Ana Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 74.)

[82] Ibidem.

[83] CUEVA, Ricardo Villas Bôas. Op.cit. p. 55. Sobre o tema, cabe ainda destacar Ana Frazão ao afirmar que "A autorregulação é essencial, portanto, para a construção de uma cultura de respeito à legalidade e à ética, uma vez que os incentivos para o cumprimento da lei passam a ser internos e desenvolvidos pela sociedade em lugar de serem externos e impostos pelo Estado." (FRAZÃO, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, André Gurnspun (Coord.) Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2017, p. 44)

Regulação e *compliance* são considerados fenômenos complementares, por intermédio da autorregulação regulada ou corregulação, os programas de *compliance* seguem preceitos estabelecidos legalmente, mas com certa discricionariedade na sua estruturação "[...] as disposições estatais estabelecem preceitos, que podem ser mais ou menos detalhados, ou criam estruturas que estimulam a autorregulação e/ou tornam vinculantes medidas de autorregulação"[84]. O Estado por intermédio de expressa previsão legal ou pela valoração da instituição de programas de *compliance*, incentiva esse ativismo por parte das empresas privadas.[85] Esta complementaridade, entre os dois mecanismos, fica bastante perceptível ao analisarmos os dispositivos contidos na LGPD, os quais foram concebidos justamente para assegurar a participação de cada agente econômico, já que em decorrência dos diversos *standards* e conceitos abertos presentes na lei, torna-se necessário a análise e contextualização à realidade fática de cada agente.[86] Diante deste panorama, atribuem-se as seguintes vantagens à adoção a programas de *compliance*:

> "(i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas –, na tutela de dados soma-se à vantagem adicional de adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD. Podem-se enumerar, ainda, benefícios, ainda que indiretos, concernentes ao desenvolvimento em qualidade e inovação, além de incrementos reputacionais."[87]

No entanto, para que tais vantagens sejam de fato auferidas é necessário que a adoção e institucionalização de programas de *compliance,* sejam de fato eficientes e respeitem aos mandamentos legais, não sendo aceitável os denominados "programas de fachada". Na verdade, a instituição de "programas de papel" ou mal concebidos, podem acarretar em penalidades mais severas.[88] Desta forma, feita esta primeira análise, em seguida, irei enumerar os principais elementos para que um programa de cumprimento seja considerado eficaz.

[84] FRAZÃO, Ana; Medeiros, Ana Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 75.

[85] Ibidem.

[86] FRAZÃO, Ana. *Compliance* de dados pessoais. Lei Geral De Proteção De Dados Pessoais e Suas Repercussões no Direito Brasileiro, 2019.

[87] Op.cit. p. 686.

[88] "Um programa de fachada, que não preencha os requisitos mínimos ou que preencha apenas formalmente, pode de fato resultar em penalidades maiores do que aquelas que seriam aplicáveis em sua ausência". (CUEVA, Ricardo Villas Bôas. Funções e finalidade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 61).

2.7 Da efetividade dos programas

De acordo com Ana Frazão, para que um programa de *compliance* seja considerado bem-sucedido este deve seguir alguns mecanismos básicos, dentre eles estão:

> "1) avaliação contínua de riscos e atualização do programa; 2) elaboração de Códigos de Ética e Conduta, que regulem a forma como se deve atuar na pessoa empresa; 3) organização compatível com o risco da atividade; 4) comprometimento da alta administração; 5) autonomia e independência do setor responsável pela supervisão do programa de *compliance*; 6) treinamentos periódicos; 7) criação de uma cultura corporativa de respeito à ética e às leis; 8) monitoramento constante dos controles e processos instituídos pelo programa de *compliance*; 9) canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes; 10) detecção, apuração e punição de condutas contrárias ao programa de *compliance*. "[89]

Importante destacar que cada empresa possui uma organização própria, sendo que os mecanismos elencados são somente recomendações para que um programa de efetividade possa ser exercido da forma mais producente o possível, respeitando as disposições legais. Buscando fornecer uma explicação concisa e mais didática o possível sobre o tema, irei elencá-los sistematicamente, condensando-os de acordo com a matéria abordada, não pretendo esgotar o tema, mas sim elenca-los e trazer uma breve explicação de sua importância.

2.7.1 Avaliação contínua de riscos e monitoramento

Para que um programa de *compliance* seja de fato efetivo e integrado a própria estrutura organizacional da empresa, é preciso que primeiramente seja realizado uma avaliação dos riscos assumidos pela empresa, identificando os seus pontos mais vulneráveis. [90] Esse é um aspecto fundamental na elaboração de um programa de *compliance*, já que sendo constatado os pontos mais fracos, dentro da organização empresarial, é possível a elaboração de um programa personalizado que atenda as especificidades da pessoa jurídica. [91]

[89] FRAZÃO, Ana; Medeiros, Ana Rafaela Martinez. p. 95.
[90] FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. p. 687 - 688.
[91] Ibidem.

Essa avaliação de riscos deverá ser realizada em todos os setores da empresa, a partir da identificação dessas fragilidades que podem acometer a pessoa jurídica.[92] A necessidade desta avaliação prévia se mostra clara ao analisarmos a definição ampla dada pela LGPD ao conceito de tratamento de dados[93]. De acordo com o posicionamento adotado pela legislação, praticamente todos os agentes econômicos estão inseridos, de alguma forma, no escopo de atuação da norma legal. No entanto, cada atividade empresarial possui as suas peculiaridades e os seus desafios, podendo variar de acordo com cada um. [94] Prevendo esta discrepância, a LGPD apresenta um importante instrumento de análise e avaliação de riscos, definindo o relatório de impacto à proteção de dados como a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (art. 5º, XVII).

Estes riscos devem ser constantemente reavaliados e atualizados à realidade da empresa, levando-se em consideração a estrutura e organização empresarial. Busca-se assim a mitigação de riscos e a correta adequação a atividade exercida. Dependendo da complexidade, os mecanismos internos deverão ser constantemente atualizados e readequados, prezando sempre pelo respeito ao efetivo cumprimento das normas que foram fixadas e a instituição de um padrão de conduta a ser seguido por todos, inibindo assim a prática de ações ilícitas.[95] Concomitantemente, é necessário que haja um monitoramento contínuo do programa, para a checagem de sua efetividade e possíveis alterações. Esses mecanismos de controle servem para assegurar que as regras estabelecidas nos Códigos de Ética e Conduta estão sendo seguidas e se existe a necessidade de alteração ou modificação.[96]

2.7.2 Dos Códigos de Ética e Conduta

[92] Idem.
[93] Considerado como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, X)
[94] FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. p. 687 - 688.
[95] Ibidem.
[96] "Paralelamente ao monitoramento, é essencial que haja também a atualização do programa de *compliance*. Identificados novos riscos, deve haver adaptação do programa. Um programa de *compliance* defasado pode acabar tornando-se inócuo. A necessidade de atualização pode decorrer de mudanças regulatórias, mas também de alterações promovidas na estratégia de negócios e/ou estrutura societária da empresa" (FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Op.cit. p. 101.)

O Código de Ética introduz as normas e princípios da empresa que deverão ser seguidos, desde os funcionários à parceiros da pessoa jurídica. Já no Código de Conduta detalha-se mais especificamente os riscos enfrentados pela empresa e as condutas que deverão ser adotadas, principalmente pelos funcionários. [97] Os códigos deverão adotar uma linguagem clara e simples, a qual seja acessível a todos os funcionários, já que eles são a parte mais vulnerável no que diz respeito ao cumprimento das normas. O objetivo principal do código é demonstrar, tanto para funcionários como para o público em geral, a importância que a pessoa jurídica dedica a observância dos preceitos legais e a criação de um ambiente de cultura corporativa.[98]

2.7.3 Comprometimento da alta administração e Cultura corporativa de *compliance*

Para que de fato a área de *compliance* seja efetiva é necessário a instituição de uma mudança cultural nas empresas. A implementação do *compliance* na empresa deve ser tido como um valor fundamental na própria cultura corporativa. [99] Para que isto seja possível, é imprescindível o envolvimento da alta direção ("Tone from the top") na implementação e incorporação do programa ao próprio dia-a-dia da empresa, incentivando de forma contínua o cumprimento aos programas de *compliance*. [100]

> "Para que a "Função de *Compliance*" seja eficaz, é necessário o comprometimento da Alta Administração e que esta faça parte da cultura organizacional, contando com o comprometimento de todos os funcionários. Todos são responsáveis por *compliance*. Um Programa de *Compliance* eficaz pode não ser o suficiente para tornar uma empresa à prova de crises. Mas certamente aprimorará o sistema de controles internos e permitirá uma gestão de riscos mais eficiente."[101]

[97] FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. p. 688.
[98] Ibidem.
[99] CADE. Guia – Programas de *Compliance* do Conselho Administrativo de Defesa Econômica. Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-*compliance*-versao-oficial.pdf. Acesso em: outubro de 2019
[100] Ibidem.
[101] ABBI - Associação Brasileira de Bancos Internacionais. Função de *Compliance*, p. 6. Disponível em: http://www.abbi.com.br/download/funcaode*compliance*_09.pdf. Acesso em: outubro de 2019

O cumprimento às normas tanto legais como éticas, deve ser internalizado no comportamento empresarial, tanto da alta administração, como dos funcionários. É somente por meio de práticas inerentes a empresa, que prezem pela ética e conformidade que o cumprimento de regras não mais será visto como um empecilho a ser vencido, mas como algo a ser buscado e valorizado.[102] Desta forma, trazendo para a realidade da LGPD, a proteção de dados pessoais deve ser tida como princípio a ser seguido e observado em toda a cadeia produtiva da organização. Diferentemente da prática aplicada anteriormente, a titularização e controle dos dados pessoais pertencem aos seus respectivos titulares, as empresas somente detém a guarda deste por um curto e específico período de tempo, entendimento este diretamente contrário as práticas empresariais atuais.[103]

Diante deste novo paradigma no cenário de proteção de dados, as estruturas empresariais deverão ser modificadas para atender a esse novo parâmetro de titularidade de dados pessoais e a sua respectiva proteção.

2.7.4 Autonomia e independência do setor responsável

Outro aspecto de fundamental importância para a efetividade do programa de *compliance*, diz respeito a sua independência e autonomia em relação aos demais setores. Os responsáveis pela execução e supervisão do programa devem ser capazes de implementar políticas, procedimentos e controles adequados, para o sucesso do *compliance*. Sendo necessário para isso, não somente, que a equipe de profissionais tenha os recursos necessários para a implementação de suas políticas, como também, que as suas decisões sejam respeitadas e cumpridas, sem a necessidade de consultoria das demais áreas.[104]

2.7.5 Treinamento periódico

[102] CADE. Guia – Programas de *Compliance* do Conselho Administrativo de Defesa Econômica.
[103] FRAZÃO, Ana. *Compliance* de dados pessoais. Op. Cit. p. 690-691.
[104] Ibidem.

O treinamento periódico aos funcionários é característica essencial para o bom funcionamento dos programas de *compliance,* já que são eles que irão lidar diariamente com as situações de risco a que se submete a empresa.[105] Entende-se que um treinamento mais direcionado às áreas de risco específicas que os funcionários estão sujeitos e as suas peculiaridades, seja a forma mais efetiva de se garantir que o programa se adeque às diversas realidades que existem dentro de uma pessoa jurídica.[106] Desta forma, os profissionais estarão mais equipados para lidar com essas situações e a empresa tem maiores garantias que o programa adotado vai ser de fato respeitado.

2.7.6 Canais de comunicação de ilícitos

Outro mecanismo de vital importância para a efetividade dos programas de *compliance*, relaciona-se a existência de meios de comunicação, os quais não somente servirão como método de controle, já que serão destinados para a apresentação de denúncias, como, talvez sendo este o seu papel principal, o de sanar dúvidas e de solicitar esclarecimentos.[107] Por óbvio que tais mecanismos serão de grande valia para a empresa tomar conhecimento de eventuais ilícitos e agir de acordo com a situação apresentada, permitindo que sejam adotadas todas as decisões cabíveis para sanar tal perigo. [108]No entanto, tem-se em consideração que tal mecanismo servirá principalmente no dia-a-dia da empresa. Servindo como ferramenta no qual os funcionários poderão sanar as suas dúvidas e questionamentos, prevenindo assim o cometimento de ilícitos e o incentivo a conformidade.

No que concerne a primeira hipótese de mecanismo de apresentação de denúncias, é necessário que se tenha todo o aporte para que a queixa oferecida por funcionários, não sejam utilizadas em sem malefício e que sejam de fato sigilosas. Este é um aspecto fundamental para o êxito deste mecanismo, caso isso não ocorra pode representar um desestímulo ao seu uso.

2.7.7 Procedimento disciplinares

Por fim, o último elemento a ser analisado refere-se aos procedimentos disciplinares a serem adotadas caso ocorra o ilícito. É importante destacar que a aplicação de eventuais punições, deverão ser destinadas a todos os integrantes da pessoa jurídica, desde os funcionários à alta administração, esse é um aspecto importante para consolidar o comprometimento da empresa com ao respeito das regras legais e éticas. Outro elemento de grande importância, é a proporcionalidade das punições com a gravidade das infrações, evitando assim possíveis abusos ou discricionariedade. As regras impostas pela empresa deverão ser claras e as suas respectivas punições conhecidas por todos, desta forma previne-se o cometimento de eventuais impunidades. [109]Esses mecanismos punitivistas, são de fundamental importância, além de demonstrar o comprometimento da organização, como também para a identificação imediata do ilícito e sua respectiva conduta para inibir que eventuais transgressões venham a ocorrer futuramente, seja adaptando ou reforçando as suas normas.

2.8 Considerações Finais

Passado as primeiras explicações tanto da Lei Geral de Proteção de Dados como sobre a função do *compliance*, iremos agora tratar da importância que este mecanismo adquire na LGPD, não somente como cláusula de diminuição de responsabilidade, mas o seu papel fundamental para a instituição de uma cultura de *compliance* a proteção de dados que tanto carece em nosso país.

[105] FRAZÃO, Ana. *Compliance* de dados pessoais. Op. Cit. p. 690-691.
[106] Ibidem.
[107] FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Op.cit. p. 101-102.
[108] FRAZÃO, Ana. *Compliance* de dados pessoais. Op. Cit. p. 692-693.
[109] MENDES, Francisco Schertel; CARVALHO, Vinicius Marques de. *Compliance*: concorrência e combate à corrupção. São Paulo: Trevisan, 2017. P. 148.

3. *COMPLIANCE* À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Diferentemente do que acontece na Europa, o Brasil conta com uma cultura de proteção de dados incipiente. Antes da aprovação da LGPD o que nós tínhamos eram retalhos de diversas legislações setoriais, que variam desde o Código de Defesa do Consumidor, do Marco Legal da Internet à Lei do Cadastro positivo, no entanto, em decorrência das discrepâncias que existiam entre elas, em muitos dos casos, acabavam por gerar entendimentos conflituosos e imprecisos, que traziam uma imensa insegurança jurídica, não somente aos titulares de dados como também para as empresas.[110] Em uma tentativa de uniformizar e preencher as lacunas presentes em nosso ordenamento surgiu a LGPD.

A partir do advento da LGPD cria-se um paradigma do controle, no qual o cidadão detém o poder sobre os seus dados, podendo deles dispor da forma como lhe convir, concedendo ou retirando o consentimento sobre o uso destes.[111] Espera-se que a partir deste empoderamento do cidadão e a institucionalização de mecanismos de controle e de supervisão sobre os seus dados, o protagonismo seja deste.

Desta forma, diante destas crescentes mudanças é fundamental uma alteração de comportamento tanto do setor público como privado, não mais prevalece o paradigma do segredo e do sigilo, tão protecionistas para com as empresas, mas sim espera-se estabelecer um novo comportamento, o qual seja mais transparente e responsável, no qual o titular de dados possua maior autonomia e as empresas maior segurança no tratamento de dados.[112]

---

[110] DONEDA, Danilo; MENDES, Laura Schertel. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, São Paulo, v. 120, p. 469- 483, nov.-dez. 2018.

[111] Ibidem.

[112] "A lei aprovada proporciona ao cidadão garantias em relação ao uso dos seus dados, a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e setor público possam utilizar esse dados pessoais, dentro dos parâmetros e limites de sua utilização. [...], introduzindo o paradigma do controle- pelo qual se garante ao cidadão o controle sobre seus dados, inclusive para que os divulgue e use, em oposição ao paradigma do segredo e do sigilo. A ideia é a de que, com o empoderamento do cidadão e com a institucionalização de mecanismos de controle e supervisão sobre o uso de seus dados, o cidadão passe a ser protagonista das decisões sobre o uso de seus dados, em linha com o conceito de autodeterminação informativa, consagrada em decisão histórica da Corte Constitucional alemã, e agora também positivado como princípio na LGPD."(DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13,709/2018): o novo paradigma da Proteção de Dados no Brasil. Revista do Consumidor, São Paulo, vol. 120, p, 22.)

3.1 Da importância do *compliance* na LGPD

Hoje, a partir da aprovação da LGPD, diferentemente da pratica adotada anteriormente, entende-se que quem é o verdadeiro titular dos dados é o cidadão, sendo assim, as empresas, para estarem em conformidade com a lei, precisaram modificar toda a forma de tratamento, coleta e utilização dos dados pessoais que eram antes empregados. [113]

Toda a perspectiva de processamento de dados foi alterada, por conseguinte, é preciso investir na transparência e na *accountability*. Isto é, todo o processo de tratamento de dados deverá ser documentado e justificado, garantindo assim uma maior prestação de contas por parte da empresa, que ficará responsável por informar os processos e meios de segurança que são utilizados, além de resguardar que as informações que foram coletadas são de fato verdadeiras e condizem com a realidade, preservando assim os direitos do titular de dados.[114]

Uma vez que as mudanças trazidas com a nova lei são diversas, o objetivo do *compliance* à LGPD é justamente servir como um mecanismo para superar esta lacuna entre lei e práticas atuais empregadas. O cenário atual de proteção de dados deverá sofrer grandes modificações nos próximos meses até a entrada em vigor da nova legislação.[115] Com o correto programa de adequação, estas mudanças não impactarão de forma tão severa as empresas, não somente por já estarem em conformidade com a lei, mas também servirá como um treinamento para as alterações que estão por vir no cenário de proteção de dados, tornando este um mecanismo fundamental para se atender corretamente as demandas exigidas pela lei.[116]

Essa necessidade de conformidade, se dá em decorrência, principalmente, da abrangência que é concedida pela LGPD à suas definições. Caracterizada pela amplitude que é concedida aos seus conceitos (tendo-se como exemplo o escopo aplicado ao que se caracteriza como dado pessoal, tratamento, entre outros), a sua aplicação será geral.[117] Em decorrência da nossa economia ser extremamente direcionada a coleta e tratamento de dados *(data driven economy)*, é praticamente impossível não se enquadrar nas hipóteses estabelecidas em lei. Desde o tratamento mais simples ao complexo, será necessária uma

[113] FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. 694.
[114] Ibidem.
[115] Idem.
[116] Idem.
[117] Idem.

adequação mínima das empresas à LGPD. A partir do momento em que ocorre a coleta de dados, seja para a identificação de um usuário à formulários a serem preenchidos na portaria de um prédio, aplica-se a legislação, não importando o tamanho da organização e para que fins esses dados serão aplicados. Com exceção dos pressupostos previstos no art. 4º, a LGPD tem aplicação ampla e irrestrita[118], impactando não somente na área consumerista e demais atividades empresariais, como também na área trabalhista e até mesmo na área da saúde.[119]

Neste momento, torna-se de extrema relevância destacar que as normas previstas na LGPD vão muito além da proteção somente do titular dos dados, mas sim de toda a estrutura em que ele está envolvido.[120] Como foi diversas vezes mencionado ao longo deste trabalho, a nossa economia atual está direcionada para a coleta e utilização de dados, no entanto, o uso indiscriminado destes dados estava pondo em risco toda a sua credibilidade para com os cidadãos, tornando-se um sistema, fadado ao fracasso, devido a sua instabilidade. Com o advento da LGPD, pretende-se conceder maior segurança não somente para os titulares de dados como também para as empresas, ao estabelecer limites para a coleta e o modo como o qual será feito, pretende-se assim estabelecer um ambiente estável e seguro para ambas as partes, no qual ambas são detentoras de direitos e deveres.[121]

Por óbvio que as empresas têm direito de coletar os dados que acharem necessário para possibilitar e fomentar o seu negócio, coibir essa pratica além de ser praticamente impossível e infrutífera, não é o intuito da legislação. O que se pretende na verdade, é garantir que esses tratamentos de dados sejam fundamentados e respeitem os preceitos legais, assegurando assim o respeito a preceitos fundamentais.[122] Isto se torna bastante claro, por exemplo, ao analisarmos o art. 50º, o qual autoriza as entidades de classe a formularem regras de boas práticas, já que em decorrência de serem conhecedoras das especificidades das empresas poderão contribuir de forma ativa para o estabelecimento dessas práticas[123].

---

[118] Vale relembrar que de acordo com art. 1º, "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

[119] Isso se torna mais claro se pensarmos no caso das contratações de empregados, nos quais os contratantes utilizam dados pessoais para admitir novos funcionários ou na área da saúde em que se utilizam dados pessoais sensíveis do paciente de forma irrestrita, abrindo espaço para possíveis atos discriminatórios.

[120] FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. 694-695.

[121] Ibidem.

[122] Idem.

[123] [...] importante papel pode ser assumido pelas entidades de classe, também autorizadas pelo art. 50 a formularem regras de boas práticas, na medida em que, conhecedoras das especificidades da atividade, podem contribuir para o estabelecimento de critérios adequados à cada hipótese, para além de traduzir preceitos legais em ações concretas a serem tomadas pelos agentes econômicos. Esses, a seu turno, beneficiar-se-iam da

Somente a partir de uma atuação ativa por parte das empresas, na estipulação de programas e boas práticas que a Lei de fato terá efetividade, já que são estes os principais agentes responsáveis pela sua concretude.

3.2 Início do programa de *compliance*

Primeiramente, é importante compreender que cada empresa possui especificidades que deverão ser levadas em consideração na elaboração de um programa de *compliance*, sendo assim não é possível montar um modelo universal o qual se adequa as necessidades particulares de todas as organizações. No entanto, existem alguns princípios que devem ser seguidos por todos para assegurar a sua adequação à lei.

Antes de adentrarmos na questão do tratamento de dados, um dos pontos essenciais a ser mencionado está no conceito do "legítimo interesse do controlador" previsto no art. 7º, inciso IX, caracterizado como hipótese autorizativa para o tratamento de dados[124]. De imediato esclarece-se que em decorrência da generalidade do conceito, característica desta Lei, a base interpretativa é considerada de certa forma ampla, sendo assim, apesar de se ter óbices de interpretação na própria legislação, presentes nos arts. 10º e 37º, os programas de *compliance* irão servir como uma espécie de complementação à LGPD[125]. Isto se torna de fundamental importância ao analisarmos os requisitos indispensáveis que deverão ser seguidos por qualquer organização antes de efetuar o tratamento de dados.

Para que o programa de *compliance* seja de fato eficaz, é necessário que sejam identificados os principais riscos aos quais a empresa está sujeita ao realizar o tratamento de

segurança decorrente da (adequada) estruturação de normas de governança fixadas pela entidade, capaz de sugerir uniformização dos padrões aplicáveis àquele mercado. A efetiva atribuição de valor a esses parâmetros por terceiros (incluindo-se a ANPD e o Poder Judiciário) é essencial para que se construa a segurança com eles pretendida. (FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. p. 697)

[124] Dentro desta linha de pensamento é importante mencionar o entendimento do RGPD sobre o tema no considerando 47 " Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade." (GENERAL Data Protection Regulation: Versão em português (de Portugal). 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em: novembro de 2019)

[125] FRAZÃO, Ana. *Compliance* de dados pessoais. Ibidem. p. 698

dados. Este é um passo essencial para a elaboração de um programa que atenda às necessidades reais da empresa, possibilitando assim a identificação dos principais riscos e empregando procedimentos que sirvam de contrapeso aos riscos enfrentados.[126] Para que haja uma correta identificação do nível de risco o qual a empresa está submetida deverá se analisar:

> "[...] (i) em que momentos há a utilização de dados pessoais; (ii) que dados são esses; (iii) como e por quem esses dados foram coletados; (iv) como a utilização desses dados se relaciona com a atividade desenvolvida; (v) o que ocorre com esses dados uma vez que ingressam e, por fim, (vi) se e como saem do controle da organização."[127]

Passada essa primeira análise, é de fundamental importância que os agentes de tratamento delimitem os fluxos de dados que estão detidos na empresa, realizando um registro de todas as atividades de tratamento realizadas (art. 37º), desde a sua coleta até a sua exclusão. Posteriormente deverá encontrar uma base legal para a necessidade de detenção daquele dado, conforme previsto no art. 7º da LGPD, além de realizar a adequação não somente dos sistemas internos da empresa, como segurança e *compliance*, como também adequar as suas políticas, contratos e demais documentos jurídicos.[128] Estes documentos poderão servir de embasamento para eventuais auditorias solicitadas pelos titulares ou pela ANPD. O Relatório de Impacto à Proteção de Dados Pessoais previsto no art. 38º, é um instrumento de importante valia para determinar esse fluxo de dados e a sua relação com a empresa, sendo fundamental na instituição de um bom *compliance*.[129] De acordo com a norma ele "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."

Esta avaliação deverá englobar de forma completa todos os processos adotados pela empresa no tratamento de dados, garantindo assim que se tenha uma visão ampla da melhor conduta a ser estabelecida pela organização, respeitando as suas especificidades. Este é um

---

126 "[...] bons programas de *compliance* baseiam-se na correta identificação dos riscos e implementação de procedimentos que a eles respondam adequada e proporcionalmente; na reavaliação periódica dos riscos, com o implemento de adaptações; no comprometimento da alta administração; na capacidade de a organização identificar e agir para minimizar os riscos; e no estabelecimento de eficientes canais de comunicação (internos e externos)." (FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. p. 699.)

127 Ibidem p. 700.

128 Idem.

129 Idem.

passo importantíssimo para o sucesso dos próximos procedimentos a serem adotados para um bom programa de *compliance*.

Após essa análise, trazendo os princípios trabalhados anteriormente no capítulo 2, podemos agora os adequar a lógica da LGPD. A partir do momento em que foram encontrados os riscos, deve-se seguir todos os preceitos relatados no capítulo anterior, quais sejam: a elaboração de um Código de Condutas (na LGPD nomeado como Boas Práticas e Governança); a ativa participação da alta administração no estabelecimento e adoção dessas práticas; a avaliação continua de riscos e monitoramento para verificar se de fato a política adotada pela empresa está sendo efetiva; além de haver uma constante reavaliação dos processos de tratamento e uso dos dados que estão mantidos na organização. Os princípios das Boas Práticas e Governança estão previstos no art. 50º, o qual estabelece os preceitos mínimos a serem seguidos pelos agentes de tratamento de dados na instituição de um programa de *compliance*[130].

Percebe-se ao analisar este artigo a importância que a Lei confere aos agentes de tratamento, principalmente ao controlador, sendo este o responsável para implementar o programa de governança em privacidade (§2º), e demonstrar o devido comprometimento da empresa com a adequação as normas de proteção de dados. Assim como foi mencionado, é de vital importância que o programa de *compliance* atenda às necessidades próprias da organização, sendo papel do controlador estabelecer um Código de Conduta que se adeque as especificidades da organização e do tipo de dados que são coletados e utilizados. Além de ser sua obrigação estabelecer políticas de segurança e acompanhamento desses dados, possibilitando o diálogo entre empresa e titular, garantindo assim uma maior transparência ao processo de tratamento de dados. Além de, por fim, ser responsabilidade exclusiva do controlador indicar um encarregado (art. 41º).

Como já mencionado, antes do advento da LGPD, os dados coletados pela empresa, a partir do momento que configuravam em sua base de dados, ficavam sob sua posse indefinidamente, sendo utilizados para diversas funções que não a que originou a coleta, sem o menor conhecimento de seu titular. No entanto, esta pratica deverá mudar, assim como

[130] Art. 50º 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.

qualquer outra coisa, os dados pessoais, possuem um ciclo de vida. Trazendo para a realidade da LGPD, para que o dado possa ser coletado ele além de ter uma finalidade especifica, também deverá ter um período certo de uso, passado o momento de sua utilidade, a empresa deverá desfazer-se deste dado, respeitando as regras de segurança previstas na legislação. Diante desta nova realidade, muda-se uma pratica que era antes padrão nas organizações de apropriação infinita dos dados coletados, colocando em riscos direitos fundamentais dos cidadãos. [131]

Partindo dessas mudanças aqui elencadas, fica claro o papel fundamental de outro elemento mencionado no capítulo anterior. Os treinamentos periódicos de funcionários serão de fundamental importância no estabelecimento dessas novas práticas de proteção de dados. Em decorrência dessas intensas transformações, será necessário implementar uma cultura de proteção de dados, algo que não é de todo presente em nossas organizações e isso somente será possível a partir de periódicos treinamentos, no qual instrui-se os funcionários para as novas práticas a serem adotadas pela empresa e as novas atitudes a serem empregadas para que a adequação a LGPD seja possível. [132]

Dentre essas novas práticas, podemos inserir o bom relacionamento que as empresas deverão ter com os titulares dos dados coletados. Esse relacionamento é de fundamental importância até mesmo no estabelecimento de um bom programa de *compliance*. [133]A LGPD incentiva a participação ativa dos titulares de dados no processamento de seus dados, isto se torna claro ao analisarmos o art. 50, §2º, inciso I e o art. 51º. Esse protagonismo também é fundamental para garantir que os titulares de dados exercem os seus direitos garantidos na LGPD, sendo na verdade um requisito na avaliação das condutas de boa governança. A empresa deve garantir não somente que os titulares possam exercer os seus direitos, mas também possibilitar que esses direitos sejam exercidos de forma informada e consciente.[134]

---

131 BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. Gen, Editora Forense, 2019.

132 FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit.

133 Ibidem.

134 Do mesmo modo afigura-se essencial que se transmita com máxima clareza todas as opções do titular quanto a eventuais dados coletados nos serviços prestados e qual o emprego lhes será dado. É salutar que se descrevam as formas por meio das quais os titulares poderão exercer os direitos garantidos pela LGPD e que se garanta a qualidade do dado, além de constar a indicação clara, expressa e destacada a respeito do encarregado pelo tratamento dos dados pessoais. A participação do titular deverá influenciar na valoração positiva das normas de *compliance* pela ANDP, 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. À evidência, deve-se ponderar quais medidas podem ser implementadas sem prejuízo do regular desempenho da atividade. (FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. p. 705).

Não somente é importante possuir um bom relacionamento com os titulares, mas também deve se ter um bom relacionamento com terceiros, seja por meio de contratação de agentes de tratamento seja com demais entidades e parceiros. É preciso que as práticas de governança permeiem todas as áreas e relacionamentos da empresa, mostrando assim o comprometimento desta ao respeito das normas legais e éticas.[135]

A LGPD estabelece também uma obrigação central dos agentes de tratamentos de dados, é a divulgação dos procedimentos adotados para a coleta e tratamento de dados, além de informar quais medidas de segurança são empregadas para garantir a inviolabilidade dos dados. Este é um passo fundamental para demonstrar a preocupação da empresa em estar em *compliance*, como também de dar maior transparência para os processos e procedimentos adotados, dando assim uma maior confiabilidade à organização e maior segurança para os titulares sobre o tratamento de seus dados. Devendo s agentes de tratamento adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (art.46).[136]

Por fim, a Lei também prevê a necessidade de programa de governança contenha um plano de reposta a incidente e remediação (art. 50, §2º, I, g), sendo esta mais uma garantia prevista na legislação para caso ocorra algum vazamento ou prática ilícita, a empresa esteja preparada para lidar em tais situações.[137] Determina-se que a partir do incidente a organização deverá comunicar a ANPD (art. 48), em prazo razoável, sendo que em tal comunicação deverá mencionar:

> "Art. 48, §1º, I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo."

O não cumprimento as regras previstas na LGPD não são uma possibilidade, pelo contrário, assim como já foi mencionada no capítulo I, as sanções impostas ao seu não cumprimento são severas e poderão impactar profundamente a reputação da empresa. Sendo

---

135 Ibidem.
136 DONEDA, Danilo; MENDES, Laura Schertel. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, São Paulo, 2018. P. 5.
137 FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit. p.710.

assim, se torna de fundamental importância que seja estabelecido programas efetivos de *compliance*.

3.3 Do papel do encarregado

Uma das principais obrigações conferida pela LGPD ao controlador, refere-se à exigência que cada empresa ou entidade que efetue tratamento de dados pessoais indique um encarregado nos termos do art. 41º, assim como já foi mencionado. O papel do encarregado, se assemelha à figura do *Data Protection Officer (DPO)*, previsto na RGPD, ele deverá ser o responsável pelo setor de *compliance* e pela sua implementação na empresa. Vale mais uma vez trazer a definição de encarregado de acordo com a LGPD "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) " (art. 5º, VIII).

Essa função, depois das alterações conferidas pela Lei nº 13.853/2019, passou a poder ser exercida tanto por pessoas físicas como jurídicas, sendo assim possível a contratação de uma figura externa ao quadro de funcionários da empresa. O papel do encarregado vai muito além de servir de elo entre o controlador, os titulares de dados e a ANPD, sendo ele o responsável por receber reclamações, comunicações, prestar esclarecimentos além de ter o papel de orientar os funcionários para as regras de boas práticas. O encarregado deverá ser a figura central de conformidade dentro da empresa, tanto para os funcionários, quanto para a alta direção.[138] Sendo assim, é imprescindível que ele tenha contato direto com o alto escalão da organização, se possível a indicação de um membro da alta administração como responsável pelo setor de *compliance* concederia maior amplitude par o instituto. Além de por fim, ser fundamental que o encarregado tenha autonomia no desempenho de suas funções.[139]

3.4 *Privacy by design*

Toda a concepção do programa de conformidade aos princípios gerais da LGPD deverá ser pensada em todo o seu desenvolvimento, garantindo-se assim desde o início, os direitos de privacidade e proteção de dados. Desta forma garantisse uma correta adequação

[138] Ibidem.
[139] Idem.

e cumprimento dos requisitos previstos na lei. Em todas as etapas desde o seu desenvolvimento à entrega do serviço ou produto, deve-se pensar na privacidade do usuário cidadão e ela deve ser respeitada.[140] É um modelo a ser seguido não somente na concepção do programa de *compliance*, mas também em aspectos do dia-a-dia, garantindo a segurança e privacidade do titular de dados. Este modelo tem dentre suas características ter natureza preventiva e proativa, procura-se evitar a ocorrência de ilícitos, desta forma se torna fundamental a avalição constante de riscos e as suas soluções.[141] De acordo com Bioni, *Privacy By Design* "é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais".[142]

Neste momento, a atuação da alta administração se torna fundamental, não somente na criação de um programa de *compliance*, mas também ao incorporara-lo e implementa-lo em todas as áreas da empresa, demonstrando através de suas atitudes a importância que a organização concede a proteção de dados, construindo assim uma cultura corporativa de respeito à LGPD.[143]

O *compliance* deve garantir não somente o respeito a regras ou princípios de comportamento, como também na aplicação de tecnologias que garantam de fato essa conformidade. A área de tecnologia vem avançado a passos antes nunca imaginados, sendo as práticas de segurança exercidas pela empresa também deverão evoluir constantemente, para que assim possa se garantir que as tecnologias empregadas sejam de fato eficientes e adequadas.[144] Importante mencionar neste momento, os ensinamentos de Bioni, o autor acredita que a tecnologia pode ser uma ferramenta para a proteção de dados pessoais, mencionando as denominadas *Privacy Enhancing Technologies* (PETs), as quais são

[140] BIONI. Bruno. Op.cit. p. 173-174. (Versão Minha Biblioteca)
[141] MULLIGAN, Deirdre K; KING, Jennifer, Bridging the Gap between Privacy and Design. University of Pennsylvania Journal of Constitutional Law, v. 14, n. 4, p. 989, 2012. Disponível em: http://ssrn.com/abstract=2070401 . Acesso em: novembro de 2019
[142] BIONI, Bruno Ricardo. Op.cit,. p. 174. (Versão Minha Biblioteca)
[143] FRAZÃO, Ana. *Compliance* de dados pessoais. Op.cit.
[144] "Daí a necessidade de que os programas de *compliance* de dados não se limitem apenas à previsão de princípios ou regras de comportamento, mas visem também à adoção de tecnologias que possam ser compatíveis com a eficácia de tais regras. É essa uma das principais preocupações decorrentes da ideia de privacy by design, em que a escolha da tecnologia utilizada na oferta de produtos e serviços é pensada, desde o início, para a proteção dos dados pessoais." (FRAZÃO, Ana. *Compliance* de dados pessoais. Ibidem. P. 710)

tecnologias que reforçam/melhoram o controle e a proteção das informações pessoais dos cidadãos.[145]

3.5 Incentivo para adoção de programas de *compliance* à LGPD

Como bem relata Ana Frazão, quantificar os benefícios decorrentes do *compliance* é complicado, no entanto, a LGPD buscou conceder um tratamento diferenciado para aqueles que adotarem programas efetivos de *compliance*. Antes de adentrar no tema propriamente dito, é importante destacar que além dos incentivos concedidos na lei, o *compliance* traz grandes vantagens econômicas e reputacionais para aqueles que o adotam, apesar de não ser exatamente possível quantifica-lo.[146] Dentre estas vantagens estão:

> "[...] (i) vantagens reputacionais, (ii) o estimulo para maior investimento em inovação e qualidade, em razão da sua supressão dos benefícios decorrentes de vantagens ilícitas, que alteram a dinâmica concorrencial, (iii) melhorias do padrão de gestão organizacional, que podem contribuir para a eficiência da empresa, (iv) aumento das oportunidades de negócio, e, por fim, (v) a própria economia decorrente da prevenção do ilícito e/ ou da minoração de seus danos." [147]

Além da aplicação de sanções para o descumprimento da norma, o legislador se preocupou em estabelecer incentivos para aqueles que de fato cumprem com a lei. No art. 52, §1º, incisos VIII e IX[148], percebe-se a importância concedida pela lei aos programas de conformidade, os quais dependendo da observância dos demais fatores previstos no parágrafo, poderão servir como atenuantes de sanções administrativas.[149] Uma vez estabelecido que foram utilizados todos os meios cabíveis a pessoa jurídica para evitar o ilícito, não deverá incidir a reprovabilidade ou culpabilidade sob suas ações, impedindo assim a aplicação de sanções.[150]

---

145 BIONI. Bruno. Ibidem p. 173. (Versão Minha Biblioteca)
146 FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Op. Cit. p.81.
147 Ibidem.
148 Art. 52. § 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:
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;
149 Frazão, Ana. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, André Gurnspun (Coord.) Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2017. P. 52.
150 Ibidem.

3.6 Novas perspectivas para o *compliance* na LGPD: autorregulação regulada

Como já mencionado no capítulo anterior, a autorregulação possui um papel fundamental para a efetividade e implementação da LGPD. Antes de adentrarmos no tema, é importante mencionar que o mercado de processamento de dados apresenta, desde a sua concepção, características tendentes à auto-organização e a autorregulação, sendo assim, antes do advento de leis de proteção de dados, o mercado de tratamento de dados já possuía regras comportamentais autodesenvolvidas.[151] No entanto, em razão dessas regras terem sido criadas unilateralmente pelas partes mais poderosas da relação, sendo estes os agentes de tratamento, sem os demais representantes das demais partes interessadas, elas possuíam como característica serem impositivas em detrimento dos demais.[152] Como uma forma de conferir maior estabilidade e equidade ao sistema, o Estado adentra a relação com um papel de garantir que as normas definidas pelo setor privada sejam cumpridas, ao estabelecer diretrizes gerais de comportamento a serem seguidas. Sobre o tema, é importante mencionar a consideração feita por Hoffmann-Riem:

> "Falo de *autorregulamentação social regulada pelo Estado*, ou, em termos breves, de *autorregulação/autorregulamentação regulada/regulamentada* quando órgãos estatais confiam, para a solução de problemas, nas ordens criadas com (relativa) autonomia pelos membros da sociedade, mas atuam regulatoriamente de modo que, quando isso é feito, (também) se observem ou persigam deliberadamente fins relacionados ao bem comum. A influência do Estado pode acontecer de forma extremamente diversificada, p. ex., na forma de normas ou estímulos comportamentais, por meio do estabelecimento de estruturas – como as de natureza corporativa – ou pela viabilização e apoio de sistemas funcionais da sociedade, como o mercado."[153]

A partir dessa cooperação entre mercado e Estado é possível estabelecer uma regulamentação híbrida, no qual "uma regulação surge pela autorregulamentação social, mas órgãos estatais participam do desenvolvimento das regras e/ou da definição de sua relevância."[154] Trazendo para o contexto da LGPD, essa parceria é imprescindível para o sucesso da regulamentação em nosso ordenamento jurídico. A partir do momento em que o mercado acolhe as alterações estipuladas por lei e as emprega em suas políticas de conduta, a implementação da regulação em nossa sociedade se torna viável.

---

[151] HOFFMANN-RIEM, Wolfgang. Autorregulação, autorregulamentação e autorregulamentação regulamentada no contexto digital. Revista da AJURIS, v. 46, n. 146, p. 529-554, 2019.
[152] Ibidem.
[153] Idem.
[154] Idem.

3.7 Desafios

A realidade brasileira no que concerne a proteção de dados ainda é muito recente e não foi estabelecida como algo a ser aspirado, ainda, por grande parte das empresas, principalmente aquelas de pequeno e médio porte. Diante deste cenário, a LGPD terá um obstáculo a mais para superar do que as demais legislações contemporâneas no que concerne a estruturação de uma cultura corporativa que age em conformidade com a lei. Os mecanismos de interpretação jurídica ainda estão sendo moldados[155] a partir das novas demandas que estão surgindo no judiciário. Com base nesse panorama as empresas terão papel inestimável para fomentar esta cultura de *compliance*, devendo então ser necessário diversos estímulos por parte do Poder Público, além de uma vigilância severa para que de fato essa nova realidade de conformidade seja exercida.

Além do estabelecimento de uma cultura de *compliance* na sociedade brasileira, outro desafio a ser enfrentado refere-se ao custo desprendido para a adoção de um programa efetivo de *compliance*. Em decorrência dos rígidos padrões estabelecidos na LGPD, os custos para o estabelecimento dos programas de integridade, dependendo da atividade exercida pela empresa e os riscos aos quais está submetido, serão altos.[156] Desta forma, para que de fato as boas práticas e governança sejam adotadas, deverão ter incentivos e estímulos para a sua adoção. Dentre tais estímulos, estão: o bom relacionamento com os titulares de dados, no qual contribui para a construção de um ambiente de confiança, algo fundamental para a boa reputação da empresa; a implementação de um programa de *compliance* serve como mecanismo para afastar ou diminuir a sua responsabilidade (art. 43º) e dar maior segurança em possíveis futuras ações; além de ser critério atenuante no estabelecimento das sanções administrativas pela ANPD.[157]

---

[155] Diante deste cenário a CGU em 2018, desenvolveu um Manual prático de avaliação do programa de integridade em PAR, com o intuito de garantir segurança e uniformidade técnica na avaliação de programas de integridade. O manual está disponível em: https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/manual-pratico-integridade-par.pdf

[156] "A implementação de programas de *compliance* impõe uma série de custos. A instituição de um programa robusto exige a contratação de especialistas, a elaboração de um código de ética e conduta, a avaliação perante dos riscos, o investimento contínuo no treinamento dos empregados, a contratação de *compliance officers externos* e de auditoria externa, o investimento em mecanismos de controle interno, inclusive em tecnologia da informação, para aprimorar os mecanismos de gerenciamento dos riscos, despesas relacionadas à manutenção do comitê de *compliance*, etc." (FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 80).

[157] "Ao fixar a metodologia da aplicação das sanções administrativas, o peso da adoção de boas práticas de governança corporativa deve ser efetivamente significativo, especialmente valorizando os programas que foram

CONCLUSÃO

A Lei Geral de Proteção de Dados, trouxe consigo grandes mudanças no cenário atual de proteção de dados. Em um mundo cada vez mais conectado, no qual os dados pessoais se tornaram insumos a serem adquiridos, a proteção do cidadão se tornou prioridade. Não somente para garantir o respeito aos preceitos constitucionais, o que por si só já é um excelente motivo, mas também e talvez esse seja o principal objetivo, regulamentar a coleta e uso de dados em nossa sociedade. A forma instável e desregulada, o qual se inseria a coleta e tratamento de dados, não era autossustentável e isso se tornou obvio para o mundo inteiro a partir das constantes violações que estavam ocorrendo, não somente na área da privacidade e autodeterminação do indivíduo, como também estava interferindo até mesmo em processos democráticos de diversos países, como vimos no caso da Cambridge Analytica.

O modelo em que seguíamos de não responsabilização e cumprimento de normas simples, simplesmente não era sustentável. A partir das mudanças realizadas pela LGPD, não só reestabelecemos a confiança dos cidadãos no mercado, como também se cria um ambiente de segurança para os agentes de tratamento de dados, ao dispor de regras claras e concisas sobre o uso e coleta de dados. Desenvolveu-se um sistema que institui a transparência e *accountability* como princípios a serem seguidos, no qual limita-se o tratamento de dados pessoais ao cumprimento de regras e princípios de gerais de adequação, e ao mesmo tempo empoderam os titulares de dados para controlar efetivamente os seus dados.

Um instituto fundamental para garantir que estes preceitos sejam cumpridos é a implementação de programas de *compliance*, os quais são mecanismos necessários para a prevenção de ilícitos e para a criação de uma cultura corporativa ética e integra, que atue ativamente na construção de ambientes compromissados com o respeito tanto ético como legal. A implementação desses programas, no entanto, é bastante onerosa, sendo é necessário que haja um efetivo incentivo por parte do Poder Público, seja na responsabilização ao restringir a punição da pessoa jurídica seja para ganho de recompensas ou vantagens, para a sua implementação e difusão. E para isso será necessário o estabelecimento de critérios rígidos para diferenciar programas de fachada com programas efetivos de *compliance*.

objeto de reconhecimento e publicização – devendo, a rigor, poder até mesmo representar a ausência de responsabilização da pessoa jurídica." (FRAZÃO, Ana. *Compliance* de dados pessoais. In.: Lei Geral de Proteção de Dados Pessoas e suas repercussões no direito brasileiro (coord. Gustavo Tepedino, Ana Frazão e Milena Donato Oliva). São Paulo: Thomson Reuters Brasil, 2019. p. 712-713).

Um bom e efetivo programa de *compliance*, deverá seguir alguns parâmetros, sendo eles:

> "1) avaliação contínua de riscos e atualização do programa; 2) elaboração de Códigos de Ética e Conduta, que regulem a forma como se deve atuar na pessoa empresa; 3) organização compatível com o risco da atividade; 4) comprometimento da alta administração; 5) autonomia e independência do setor responsável pela supervisão do programa de *compliance*; 6) treinamentos periódicos; 7) criação de uma cultura corporativa de respeito à ética e às leis; 8) monitoramento constante dos controles e processos instituídos pelo programa de *compliance*; 9) canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes; 10) detecção, apuração e punição de condutas contrárias ao programa de *compliance*."

Mas é importante salientar que estes são somente princípios orientadores para a criação de um bom programa de *compliance*, cada organização tem uma realidade própria e isto deve ser levado em consideração a instituição dos programas de adequação, caso contrário a sua efetividade pode ser compromissada, já que caso não haja a identificação por parte dos envolvidos na empresa estes pouco provavelmente irão seguir um programa que não se adeque a sua realidade.

Por fim, em decorrência da particularidade da LGPD, os métodos adotados para a sua adequação também deverão ser especificamente criados para função. Os conceitos de privacidade e proteção de dados deverão ser princípios a serem seguidos desde a concepção do programa até a sua execução, garantindo assim que os preceitos estipulados sejam de fato seguidos. Em decorrência da constante mutabilidade da disciplina de proteção de dados, os programas de integridade também deverão seguir esta característica.

A LGPD trouxe consigo grandes mudanças para o cenário de proteção de dados pessoais brasileiro, até a sua efetiva implementação em nosso ordenamento, as organizações deverão realizar mudanças drásticas no tratamento concedido a proteção de dados. Temos um longo caminho a percorrer até que de fato tenhamos uma cultura de *compliance*, mas os primeiros passos já foram dados. Espera-se que a partir das mudanças ocasionadas com a LGPD tenhamos uma nova sociedade da informação do Brasil, com cidadãos empoderados e uma segurança maior no tratamento de dados pessoais.

REFERÊNCIAS

ABBI - Associação Brasileira de Bancos Internacionais. Função de *Compliance*. Disponível em: http://www.abbi.com.br/download/funcaode*compliance*_09.pdf. Acesso em: outubro de 2019

AGUILERA, Ruth V. et al. Connecting the dots: Bringing external corporate governance into the corporate governance puzzle. The Academy of Management Annals, v. 9, n. 1, p. 483-573, 2015.

BERTOCCELLI, Rodrigo de Pinho. *Compliance*. In: VENTURINI, Otavio Venturini et al (Coord.). Manual de *Compliance*. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. Gen, Editora Forense, 2019.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado, 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. LEI Nº 13.709, de 14 de agosto de 2018. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). Brasília: Congresso Nacional, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: novembro de 2019

CADBURY COMMITTEE. The report of the committee on financial aspects of corporate governance. Londres: Cadbury Committee, Dec. 1992.

CADE. Guia – Programas de *Compliance* do Conselho Administrativo de Defesa Econômica. Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-*compliance*-versao-oficial.pdf. Acesso em: outubro de 2019

CGU. Manual prático de avaliação do programa de integridade em PAR. Diponivel em: https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/manual-pratico-integridade-par.pdf . Acesso em: novembro de 2019

CUEVA, Ricardo Villas Bôas. Funções e finalidade dos programas de *compliance*. IN: Cueva, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 53-69.

DANAHER, J. (2016). "Algorithmic decision-making and the problem of opacity". SCL. Disponível em: https://www.scl.org/articles/3713-algorithmic-decision-making-and-the-problem-of-opacity. Acesso em: setembro de 2019

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 11.

_____. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo; MENDES, Laura Schertel. Comentário à nova Lei de Proteção de Dados (Lei 13,709/2018): o novo paradigma da Proteção de Dados no Brasil. Revista do Consumidor, São Paulo, vol. 120, p, 555-587, nov. - dez. 2018.

_____. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, São Paulo, v. 120, p. 469- 483, nov.-dez. 2018.

FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial, Parte I. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018 . Acesso em: setembro de 2019

_____. *Compliance* de dados pessoais. In.: Lei Geral de Proteção de Dados Pessoas e suas repercussões no direito brasileiro (coord. Gustavo Tepedino, Ana Frazão e Milena Donato Oliva). São Paulo: Thomson Reuters Brasil, 2019.

_____. Nova LGPD: direitos dos titulares de dados pessoais. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-os-direitos-dos-titulares-de-dados-pessoais-17102018 . Acesso em: setembro de 2019

_____. Programas de *compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, André Gurnspun (Coord.) Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2017.

FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance:* perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

GANGADHARAN, Seeta Peña. Digital inclusion and data profiling. Disponível em: http://firstmonday.org/ojs/index.php/fm/article/view/3821/3199 . Acesso em: agosto de 2019.

GENERAL Data Protection Regulation: Versão em português (de Portugal). 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT . Acesso em: novembro de 2019

HOFFMANN-RIEM, Wolfgang. Autorregulação, autorregulamentação e autorregulamentação regulamentada no contexto digital. Revista da AJURIS, v. 46, n. 146, p. 529-554, 2019.

IBGC (2018). *Código das melhores práticas de governança corporativa,* p. 20. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138. Acesso em: outubro de 2019.

MENDES, Francisco Schertel; CARVALHO, Vinicius Marques de. *Compliance*: concorrência e combate à corrupção. São Paulo: Trevisan, 2017.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Editora Saraiva, 2014.

MULLIGAN, Deirdre K; KING, Jennifer, Bridging the Gap between Privacy and Design. University of Pennsylvania Journal of Constitutional Law, v. 14, n. 4, p. 989, 2012. Disponível em: http://ssrn.com/abstract=2070401 . Acesso em: novembro de 2019

NISSENBAUM, Helen. Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press, 2009.

O'NEIL, Cathy. Weapons of math destruction: How big data increases inequality and threatens democracy. New York: Crown, 2016.

OLIVIA, Milena Donato; SILVA, Rodrigo da Guia. Origem e evolução histórica do *compliance* no direito brasileiro. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 29-51.

PASQUALE, Frank. The black box society. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

ROSSETTI, José Paschoal; ANDRADE, Adriana. Governança corporativa: fundamentos, desenvolvimento e tendências. 7. ed. São Paulo: Atlas, 2014.

SILVA, C. Edson. Governança corporativa nas empresas. 4. ed. São Paulo: Atlas, 2019.

STAIR, Ralph; REYNOLDS, George W. Princípios de sistema de informação: uma abordagem gerencial. Tradução Flávio Soares Correa. São Paulo: Cengage Learning, 2009.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, v. 30, n. 1, p. 75-89, 2015.

_____. The age of surveillance capitalism. The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.