UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

A IMPLEMENTAÇÃO DA LEI 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS E OS IMPACTOS NO SETOR EMPRESARIAL

MILENA RAMALHO MORAES DA SILVA

RIO DE JANEIRO
2021

MILENA RAMALHO MORAES DA SILVA

A IMPLEMENTAÇÃO DA LEI 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS E OS IMPACTOS NO SETOR EMPRESARIAL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Enzo Baiocchi.

Rio de Janeiro

2021

Ficha catalográfica

MILENA RAMALHO MORAES DA SILVA

A IMPLEMENTAÇÃO DA LEI 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS E OS IMPACTOS NO SETOR EMPRESARIAL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Enzo Baiocchi.

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

_____

Orientador

_____

Co-orientador (Opcional)

_____

Membro da Banca

_____

Membro da Banca

Rio de Janeiro

2021

RESUMO

O presente trabalho objetiva estudar a aplicabilidade da Lei Geral de Proteção de Dados no Brasil e as discussões envolvendo suas disposições e seus impactos na sociedade brasileira, especialmente, dentro do mundo jurídico e com relação às atividades desempenhadas pelas empresas privadas.

Nesse sentido, busca-se compreender conceitos e instrumentos relevantes adotados pela legislação, principalmente o seu aspecto metodológico de abordagem de gerenciamento de riscos, que visam além da proteção de dados pessoais, preponderar os interesses mercadológicos de tecnologia e inovação que envolve o tratamento de dados pessoais no setor empresarial.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais no Brasil, Atividade Empresarial, Big Data, Mineração de Dados, Relatório de Impacto de Proteção de Dados Pessoais.

SUMÁRIO

I - INTRODUÇÃO

A presente pesquisa acadêmica tem como objetivo entender a aplicabilidade da Lei Geral de Proteção de Dados (LGPD) no ramo empresarial, tendo em vista os deveres específicos criados aos empresários e as respectivas sanções no descumprimento. Busca-se analisar não somente à relação de proteção de dados pessoais e a privacidade de seu titular, mas também a postura das empresas no tratamento de dados, para prevenir vazamentos indesejados, bem como oferecer segurança de informação aos seus clientes e usuários.

Em um contexto histórico, as transformações na sociedade sempre foram marcadas por eventos que alteraram significativamente a sua ordem social e econômica. Com o advento das novas tecnologias e a Internet, o processamento de dados recebeu a denominação de novo petróleo, em razão do seu grande valor econômico para desenvolver tecnologias avançadas. No âmbito das empresas, é um elemento fundamental para estudos analíticos e comportamentais, bem como para produção de produtos e serviços.

Devido à grande importância do tratamento de dados pessoais nas atividades econômicas, vê-se a necessidade de leis para regulamentar o uso desses dados pessoais, principalmente para preservar a privacidade e os direitos inerentes ao indivíduo. Com o marco histórico da regulamentação europeia, a RGPD, o Brasil implementa a Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que visa regulamentar o tratamento e a proteção de dados pessoais no ordenamento brasileiro.

O que se pretende nessa pesquisa é elucidar termologias do tratamento de dados, bem como entender a importância desses dados no desenvolvimento de novas tecnologias e inovação. Na esfera normativa, busca-se compreender o contexto histórico até a criação da Lei Geral de Proteção de Dados Pessoais, observando os fundamentos e princípios.

A LGPD, em sua redação, adota uma metodologia de autorregulação para avaliar os riscos do tratamento de dados nas empresas. Dessa forma, apresenta medidas e práticas de políticas internas para que as empresas façam a coleta e uso de dados, em conformidade com os trâmites legais. Além de estabelecer limites e parâmetros para o tratamento de dados, cria um órgão fiscalizador, que vai supervisar a adequação das empresas.

.

A presente pesquisa será desenvolvida através do método dialético, empregando, para tanto, uma abordagem necessariamente qualitativa quando da análise do objeto desta pesquisa jurídica, utilizando-se da bibliografia pertinente à temática em foco, com respaldo na legislação, na doutrina, a fim sustentar a sua tese.

1. O impacto da sociedade informacional nas atividades empresariais

O Código Civil de 2002, o qual adotou o fundamento da Teoria da Empresa, conceitua o empresário como "aquele que exerce profissionalmente atividade econômica organizada para produção ou circulação de bens."[1]. Nesse sentido, compreende-se que a empresa é a atividade econômica, e o sujeito que explora profissionalmente essa atividade é denominado de empresário (pessoa física) ou sociedade empresária (pessoa jurídica).

Segundo Fábio Ulhoa[2], a função social da empresa é gerar empregos, tributos e riquezas, visando contribuir para o desenvolvimento econômico, social e cultural da comunidade, de sua região ou do país, adotando práticas empresariais sustentáveis com objetivo de proteção ao meio ambiente e ao consumidor. Destaca ainda que:

> "*Se sua atuação é consentânea com estes objetivos e se desenvolve com estrita obediência às leis a que se encontra*

[1] **Código Civil:** "Art. 966: Considera-se empresário quem exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços."

[2] COELHO, Fabio Ulhoa. Curso de Direito Comercial, volume 1: direito de empresa..20.ed.São Paulo: Editora: Revistas dos Tribunais, 2016, p.76

> *sujeita, a empresa está cumprindo sua função social; isto é, os bens de produção reunidos pelo empresário na organização do estabelecimento empresarial estão tendo o emprego determinado pela Constituição Federal*".

Constituição Federal, por sua vez, destaca que a função social da propriedade no aspecto principiológico, e por consequência da empresa, é garantir que os direitos à propriedade, da livre iniciativa, e concorrência, sejam exercidos em harmonia com os direitos individuais e os interesses da coletividade, nos termos do art. 5°, XXIII e art. 170[3]. Nesse sentido, Fábio Soares [4], destaca:

> *"[...] o princípio da função social é resultante da ideia de solidariedade do Estado Democrático de Direito e nesse sentido determina que os indivíduos devam exercitar as suas liberdades em prol da coletividade, objetivando a todos os indivíduos existência dignas*"

Dado a concepção de empresa, empresário e a função da empresa, salienta-se abranger o desenvolvimento das atividades econômicas ao longo do tempo. Ao descrever a empresa como atividade, depreende-se que toda atividade econômica está necessariamente inserida em um contexto social[5], que está atrelada à interação entre as pessoas na busca por lucro e à positivação de regras que pudessem conferir segurança jurídica aos agentes econômicos[6].

---

[3] Constituição Federal de 1988: "**Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XXIII - a propriedade atenderá a sua função social; e Art. 170: "
Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: III - função social da propriedade;

[4] SOARES, Fábio Lopes. Governança cidadã: alternativa para garantia da realização da função social das empresas e de sustentabilidade econômica. **Revista da Faculdade de Direito de São Bernardo do Campo**, São Bernardo do Campo, v. 22, n. 1, p. 1-16, 2016.

[5] COELHO, Fabio Ulhoa. Curso de Direito Comercial, volume 1: direito de empresa.20. ed. São Paulo: Editora: Revistas dos Tribunais, 2016, p.50

[6] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.13

A contínua transformação da sociedade, reflete no surgimento de novos modelos de negócios, assim como, nos remete à reformulação da produção, do consumo, e dos sistemas[7]. Segundo Klaus Schwab, o uso de novas tecnologias desencadeou uma alteração profunda nas estruturas sociais e nos sistemas econômicos. Sendo historicamente três importantes revoluções: a) A revolução agrícola, que ocorreu por volta de 10.000 anos atrás e utilizou a força dos animais e a dos seres humanos para trazer melhorias de produção e urbanização nas cidades; b) A Primeira Revolução Industrial, (segunda metade do século XVIII), que transitou o uso da força muscular para energia mecânica; e por fim c) A Segunda revolução industrial (final do século XIX, e início do século XX), advém da eletricidade e a linha de montagem para produção em massa. Essa última, impulsionada também pelo desenvolvimento de computação e internet (nas décadas de 1980 e 1990).

Nesse contexto, o autor Segundo Klaus Schwab[8], dispõe que a Quarta Revolução Industrial, a qual estamos vivenciando, é uma revolução tecnológica que modifica fundamentalmente as atividades da sociedade, por meio de inteligência artificial, robótica e a internet das coisas.

Essa sociedade, também conhecida como a Sociedade Informacional ou Sociedade da Informação, depreende-se da produção de dados e informações de quantidade imensurável.[9]

Define nestes termos, a Sociedade de Informação do Brasil:

> "*A sociedade da informação não é um modismo. Representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um novo paradigma técnico-econômico. É um fenômeno global, com elevado potencial transformador das atividades sociais e*

[7] SCHWAB, Klaus. **A Quarta Revolução Industrial.** Rio de Janeiro: EDIPRO, 2019. p.15

[8] SCHWAB, Klaus. **A Quarta Revolução Industrial.** Rio de Janeiro: EDIPRO, 2019.

[9] Castells, M. (2002). A Era da Informação: Economia, Sociedade e Cultura, Vol. I,A Sociedade em Rede. Lisboa: Fundação Calouste Gulbenkian

> *econômicas, uma vez que a estrutura e a dinâmica dessas atividades inevitavelmente serão, em alguma medida, afetadas pela infraestrutura de informações disponível. É também acentuada sua dimensão político-econômica, decorrente da contribuição da infraestrutura de informações para que as regiões sejam mais ou menos atraentes em relação aos negócios e empreendimentos. Sua importância assemelha-se à de uma boa estrada de rodagem para o sucesso econômico das localidades. Tem ainda marcante dimensão social, em virtude do seu elevado potencial de promover a integração, ao reduzir as distâncias entre pessoas e aumentar o seu nível de informação."*[10]

Logo, ressalta-se os impactos desta sociedade de informação, tanto para as atividades empresariais, quanto para o Estado, que além do consumo de dados, também controla o fluxo de informações.

2. Conceito de Big data e Mineração de Dados

Para entender melhor a relação de dados, informações, e a mineração para utilização das empresas, é necessário compreender o tratamento desses dados pessoais e a forma que devem ser processados, sem ultrapassar os limites da privacidade da vida das pessoas.

Compreende-se por tratamento de dados pessoais, extraído do art. 5°, X, da LGPD, 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"*[11]

[10] SOCIEDADE DA INFORMAÇÃO NO BRASIL, 2000, p. 5
[11] Lei Geral de Proteção de Dados Pessoais.

Nessa ótica, o termo *Big Data* refere-se ao grande volume de dados brutos, não agregados, não organizados, gerados em alta velocidade e variedade, que necessitam de tratamento para serem valorados, organizados e armazenados. O volume desses dados admite a realização de análises computadorizadas e a extração de informações que jamais seriam alcançadas de forma manual.[12]Neste sentido, Ana Frazão, observa:

> *"Para entender a importância do big data para a concorrência, é importante entendermos que os dados se diferenciam da informação e do conhecimento. Colocada a questão de forma bastante simplificada, os dados podem ser considerados como matérias-primas da informação e a informação pode ser considerada importante matéria-prima do conhecimento, visto este como o resultado de uma reflexão mais consistente – e preferencialmente suscetível de aplicação – a respeito de informações sobre determinada área ou assunto"*[13]

Outrossim, Ana Frazão, dispõe que para agregar valor ao mercado, os dados precisam ser processados de maneira eficiente e rápida, visto que sem esse procedimento, não é possível transformá-los em informação:

> *"Os dados precisam, portanto, ser processados e trabalhados para que possam gerar valor. Se tal constatação não afasta a importância em si dos dados isolados ou "crus", tem o importante papel de realçar o fato de que o mero acesso à dados, sem a possibilidade efetiva e eficiente de transformá-los*

[12] MICKENSEY&COMPANY. Big Data, Analytics, and the Future of Marketing Sales. New York: McKinsey&Company, 2013.
[13] FRAZÃO, Ana. **Plataformas digitais e os desafios para a regulação jurídica**. v.1. Belo Horizonte: Editora D'Plácido, 2018.

> *em informação, pode ser insuficiente para a obtenção dos respectivos benefícios econômicos."*[14]

A mineração de dados consiste na interpretação das informações coletadas, além de tudo, é por meio desse processo (dados que contém informações sobre os hábitos e interesses dos indivíduos), que as empresas vão usar como referência para avaliar suas ações, e gerar conhecimento para tomada de decisão.

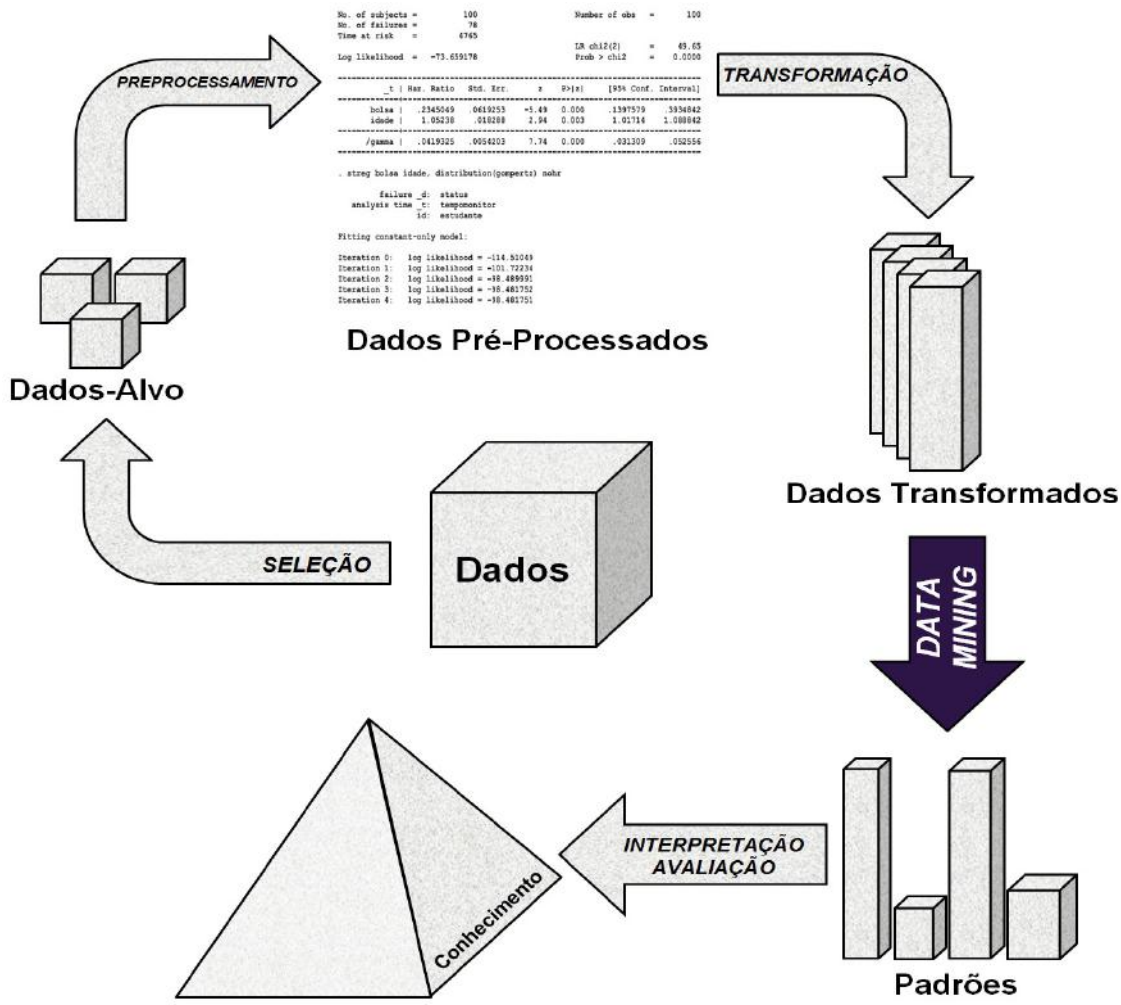
Em outras palavras, a mineração de dados é uma técnica, um reconhecimento de padrões, otimização, simulação, estatística e análise multivariada para encontrar padrões a partir dos dados. Na etapa do processo do KDD representa a aplicação de algoritmos de análise e descoberta de dados que, padrões (ou modelos) sobre os dados.

Para entender as fases de um processo de mineração de dados, na figura 1, temos um exemplo visual do chamado KDD (*Knowlegde Discovery in Datasets*) e o *Data mining*, que muitas vezes são vistos como sinônimos:

Figura 1 – Ciclo de um processo KDD e Data mining[15]

[14] FRAZÃO, Ana. **Plataformas digitais e os desafios para a regulação jurídica**. v.1. Belo Horizonte: Editora D'Plácido, 2018

[15]Disponível em: https://www.itforum365.com.br/wp-content/uploads/2019/04/Figura-KDD-e-Data-Mining.png Acesso em 23/09/2021



Fonte: Fayyad, Piatetsky-Shapiro e Smyth. **From data mining to knowledge discovery in databases.**

As etapas[16] para mineração de dados, conforme Larose e Larose, *Discovering Knowledge in Data: An Introduction to Data Mining*[17]:

1 – Entendimento dos Negócios: Nessa fase, busca-se o conhecimento sobre o negócio e sobre os inerentes processos mercadológicos é de fundamental para entender os objetivos da mineração de dados. E guiará as próximas etapas.

[16] Disponível em: https://itforum.com.br/coluna/kdd-e-data-mining-mais-do-que-apenas-conceitos/. Acesso em 21/09/2021

[17] LAROSE, D. T. Discovering Knowledge in Data: An Introduction to Data Mining. John Wiley and Sons, Inc, 2005

2 – Entendimento dos Dados: Os dados vêm de diversas fontes, portanto, deve-se descrever e identificá-los com bastante clareza, sempre explicitando as diversas fontes de obtenção e eventuais comportamentos de interdependência entre variáveis.

3 – Preparação dos Dados: Os dados (pelas inúmeras fontes) nem sempre estão preparados para o método de mineração. Por isso, é necessário análises preliminares dos dados, com eventuais tratamentos, a fim de auxiliar os métodos de data mining, e para que sejam aplicados corretamente. O próprio agrupamento de variáveis ou a categorização por meio de determinado critério pode tornar uma técnica mais adequada do que outra, respeitando os objetivos da análise.

4 – Modelagem: Essa é a fase em que as técnicas (algoritmos) de mineração serão aplicadas. Diversas técnicas podem ser determinadas: como a elaboração de técnicas exploratórias, a estimação de modelos confirmatórios ou a implementação de algoritmos, sempre com base nos objetivos propostos.

5 – Análise dos Resultados (avaliação): Nessa fase, é essencial que participem tanto conhecedores do negócio quanto estatísticos e especialistas nos dados, a fim de que sejam elaboradas avaliações sobre os achados na etapa anterior, a partir da análise de testes e validações.

6 – Divulgação dos Resultados(distribuição): Na fase final, é o resultado e entendimento das informações coletadas após todos os procedimentos, é importante que os envolvidos tenham ciência dos resultados, a fim de que seja possível a implantação de procedimentos de gestão.

Visto que o procedimento para transformar dados em conhecimento e conteúdo, resultando em valor para os novos modelos de negócios, é primordial entender as informações intrínsecas que podem vir com esses dados, principalmente àqueles pessoais e sensíveis.

3. Dados Pessoais como elemento da empresa

A coleta de dados e informações permite as mais detalhadas análises de comportamento dos seus usuários, bem como de seus consumidores. Além disso, com base nessas informações surgiu a possibilidade de explorar um novo setor de serviço, o gerenciamento de relacionamento com o cliente, (*Customer Relationship Management* – CRM). Por CRM, entende-se:

> "CRM são as iniciais de Customer Relationship Management (Gestão de Relacionamento com o Cliente). O termo se refere a um conjunto de práticas, estratégias de negócio e tecnologias focadas no cliente que, desde pequenas e médias, até grandes empresas, podem utilizar para gerenciar e analisar as interações com seus clientes, antecipar suas necessidades e desejos, otimizar a rentabilidade e aumentar as vendas e a assertividade de suas campanhas de captação de novos clientes. O CRM armazena informações de clientes atuais e potenciais – nome, endereço, número de telefone etc. –, e suas atividades e pontos de contato com a empresa, incluindo visitas a sites, ligações telefônicas, e-mails, entre outras interações. Entretanto, a plataforma não é apenas uma lista de contatos elaborada: ela reúne e integra dados valiosos para preparar e atualizar suas equipes com informações pessoais dos clientes, histórico e preferência de compras". SALESFORCE. O que é CRM?"[18]

Sendo assim, a utilização do processamento de dados nas atividades empresariais vislumbra um importante valor de mercado[19], sendo explorada pelos empresários no segmento de suas empresas.

Um dos exemplos de o processamento de dados ou *data mining*, que agregam valor no âmbito das empresas, é apresentado por Kenneth Laudon e Jane Laudon:

> "As associações são ocorrências ligadas a um único evento. Por exemplo: um estudo de modelos de compra em supermercados pode revelar que, na compra de salgadinhos de milho, compra-se também refrigerante tipo cola em 65% das vezes, mas, quando há uma promoção, o refrigerante é comprado em 85% das vezes. Com essas informações, os gerentes podem

[18] Disponível em: <https://www.salesforce.com/br/crm/>. Acesso em: 19/09/2021

[19] MAYER-SCHONBERGER, Viktor; CUJIER, Kenneth. Big Data: Como extrair volume, variedade e valor da avalanche de informação cotidiana. Tradução de Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013. p.70.

> tomar decisões mais acertadas pois aprenderam a respeito da rentabilidade de uma promoção.
> Na sequência, os eventos estão ligados ao longo do tempo. Pode-se descobrir, por exemplo, que quando se compra uma casa, em 65% das vezes se adquire uma nova geladeira no período de duas semanas, e que em 45% das vezes, um fogão também é comprado um mês após a compra da residência.
> A classificação reconhece que descrevem o grupo ao qual o item pertence por meio do exame dos itens já classificados e pela inferência de um conjunto de regras. Exemplo: empresas de operadoras de cartões de crédito e companhias telefônicas preocupam-se com a perda de clientes regulares, a classificação pode ajudar a descobrir as características de clientes que provavelmente virão abandoná-las e oferecer um modelo para ajudar os gerentes a prever quem são, de modo que se elabore antecipadamente campanhas especiais para reter esses clientes.
> A aglomeração (clustering) funciona de maneira semelhante a classificação quando ainda não foram definidos grupos. Uma ferramenta de data mining descobrirá diferentes agrupamentos dentro da massa de dados. Por exemplo, ao encontrar grupos de afinidades para cartões bancários ou ao dividir o banco de dados em categorias de clientes com base na demografia e em investimentos pessoais.
> Embora todas essas aplicações envolvam previsões, os prognósticos as utilizam de modo diferente. Partem de uma série de valores existentes para prever quais serão os outros valores, Por exemplo, um prognóstico pode descobrir padrões no dados que ajudam gerentes a estimar o valor futuro de variáveis com números de vendas."[20]

Ora, destaca-se, que os exemplos mencionados, mostram com clareza a diferença que as informações quando devidamente tratadas agregam valor e lucro às empresas, e por isso, em termos mercadológicos, é quase impossível uma empresa não dispor de alguns desses mecanismos. Aliás, estima-se que o não manuseio deste processamento afetará no desaparecimento das sociedades empresárias de médio porte, tendo em vista que perderão competitividade diante de grandes sociedades empresárias.[21]

Logo, surgiu a percepção que os dados pessoais como elemento de empresa, Pedro Marcos[22], denota essa relação de dados e o consumidor/cliente, começa através do empresário estabelecimento comercial da internet, seu aviamento, e à grande receita que os dados desses consumidores injetaram na empresa da nova economia:

> "*o aviamento tem como um dos seus elementos o consumidor, ou melhor, os dados desse consumidor. Para o*

[20] LAUDON, Kenneth; LAUDON, Jane. Sistemas de Informações Gerenciais. 9.ed. Tradução de Luciana do Amaram Teixeira. São Paulo: Pearson Prentice Hall, 2010.p.159
[21] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.15
[22] BARBOSA, Pedro Marcos Nunes. *E-stabelecimento*: Teoria do estabelecimento comercial na Internet, aplicativos, websites, segregação patrimonial, , trade dress eletrônico, concorrência online, ativos inatingíveis cibernéticos e negócios jurídicos. São Paulo: Quartier Latin, 2017.p.43

> *desenvolvimento de suas técnicas de colheita de dados, o largo escaneamento de obras permitiu que desenvolvessem seus algoritmos para a leitura de semiótica avançada, podendo, inclusive, compreender padrões de linguagem e prever o que o usuário espera nas suas buscas*".

No entanto, com a expansão dos dados e informações, sobretudo nas redes sociais, e consequentemente o uso nas empresas, surge a grande preocupação sobre a privacidade dos usuários e consumidores sobre as informações coletadas. Uma vez que, muitas vezes essa coleta de dados é feita sem o devido consentimento, e sua finalidade é desconhecida.

Mas, antes de entender a privacidade e seus principais aspectos, é essencial saber o que são esses dados. Por dados, a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) define os seguintes termos:

> "Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"[23]

Conforme extrai-se do Art. 5° LGPD, o dado pessoal, após o procedimento de tratamento, é aquele que as informações do cidadão serão identificadas, têm-se diretamente aquela relação da informação com a pessoa natural, como nome, endereço, endereço de e-mail etc. Diferentemente quando estamos diante dos dados anônimos, tendo em vista que estes as informações não vão ser relacionadas a uma pessoa.

[23] Lei de Proteção de Dados Pessoais, Art. 5°.

Em contrapartida, os dados sensíveis, refere-se aos dados mais íntimos da pessoa, através desses dados identificamos a origem racial ou ética, a opinião política, convicção religiosa, dados genéticos ou biométricos, dados referentes a saúde, vinculado a uma pessoa natural. Neste cenário, observamos que os dados possuem um caráter mais íntimo sobre a pessoa, logo, se mal utilizados, e eventualmente vazados, podem causar um dano ao titular daquelas informações.

À vista disso, a utilização de dados pessoais feita pelas empresas, além do consentimento do titular, necessitam de fato, de segurança de informação. Uma vez que o vazamento de dados pode provocar manchar reputacionais e abalo de confiança por parte do mercado.[24]

Contudo, conforme apresentado anteriormente, o manuseio desses dados tornou-se fundamental para o ramo empresarial, seja para descobrir uma nova tendência do mercado, ou para atender uma demanda recorrente do consumidor. Nestas palavras, Cabral diz:

> "Ao agregar a visão do consumidor à cadeia de produção, o empresário personaliza ao máximo o seu produto. Essa interação permite a redução de custos em esforços de publicidade, venda, estoque, pesquisa e desenvolvimento. Com base nas informações extraídas dos consumidores, os produtos *on demand* são feitos em pequena escala e já saem da fábrica com a venda "garantida".
> Em suma, a utilização de dados pessoais está presente em diversos aspectos da vida empresarial. Os dados são imprescindíveis para a organização da sociedade, destacando-se o necessário tratamento de informações de funcionários, fornecedores e clientela, e possuem extrema relevância para a interação e manutenção da clientela (por meio de publicidade dirigida, medidas de segurança da informação e a eventual participação do consumidor na cadeia de produção)."[25]

Isto posto, depreende-se que a utilização de dados é imprescindível para continuação das atividades empresariais. A partir dessa coleta de informações, as empresas adequam seus serviços, e desenvolvem seus negócios. No entanto, conforme veremos a seguir, as empresas precisam respeitar princípios pilares de privacidade e direitos de personalidade ao manusearem dados, principalmente àquelas sensíveis.

---

[24] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.17

[25] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019.

4. Privacidade x Proteção de Dados

Constituição Federal de 1988, no art. 5°[26], inciso X, prevê a proteção à intimidade, a privacidade, à honra e à imagem dos indivíduos, como direitos personalíssimos. Outrossim, no inciso XII do art. 5°, por sua vez, vai prever um sigilo de comunicações, seja telegráfica, de dados ou telefônicas. Esses são alguns fundamentos, ainda que muito amplos, que o ordenamento brasileiro trouxe ao denominado direito à privacidade.

Em um contexto histórico, antes de um estudo mais aprofundado sobre o conceito de privacidade, esta era atrelada como alguma forma de isolamento, o indivíduo era visto como fechado ao mundo exterior, e solitário em seu interior. Maria Celina, acentua: *"Nesta concepção o homem era visto como um ser hermeticamente fechado ao mundo exterior, isolado, solitário em seu interior. Era o chamado homo clausus, cujo melhor representante foi o personagem criado por Daniel Defoe em 1719, Robinson Crusoe"*[27]

Contudo, esse entendimento de privacidade como um direito de isolamento, foi superado pelos autores Warren e Brandeis[28], que dispuseram a privacidade como o "direito de ser deixado em paz", sem a interferência do Estado na esfera privada individual. No clássico artigo "The Right to Privacy", destaca-se que reconhecidas modificações políticas, sociais e econômicas, a natureza e redefinições da privacidade do indivíduo vão se readaptar, mas o denominador comum da privacidade permanecerá o mesmo, que ceder a privacidade, mas diante de uma justificativa legítima.

---

[26] Constituição Federal: "**Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

[27] MORAES, Maria Celina Bodin de. Na Medida da Pessoa Humana -Estudos de direito civil constitucional. Rio de Janeiro: RENOVAR, l2010, p. 140.

[28] WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy.** Harvard Law Review, Vol. 4, Nº. 5. 1890, p. 193-220.

Segundo Rodotá[29], denota-se que em uma sociedade de mídias sociais, *e-commerces*, dos aplicativos, jogos e *startups* os dados estão se proliferando em um ritmo alarmante. O desenvolvimento das tecnologias de informação está em direção oposta à manutenção das esferas privadas pessoais e de autodeterminação informativa, o que acarreta dificuldade para controlar a circulação e tratamento desses dados. O autor enfatiza que os efeitos da sociedade de informação, é o indivíduo "ceder" suas informações para usufruir desse modelo de sociedade.

De acordo com Danilo Doneda[30], a influência desta sociedade informacional, vai determinar a privacidade como aquela que busca pela igualdade, a liberdade de escolha, o anseio pela não discriminação, uma ideia ligada à personalidade[31]. De certa forma, neste caso, a privacidade muita mais ampla, e ao mesmo tempo, interligada com a subjetividade de cada indivíduo.

Por este ângulo, a concepção de privacidade migra de isolamento para o denominado direito à autodeterminação informativa, que vai garantir ao cidadão, em sua capacidade civil plena**,** o controle de suas próprias informações, em especial os dados sensíveis. Nessa linha, este **"controle"** para a circulação de seus dados, é entendido como o direito à proteção de dados pessoais.

Nesta perspectiva, Laura Schertel Mendes aduz:

> "Como pode-se perceber, a partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais. Nesse contexto, percebe-se uma alteração não apenas do conteúdo do direito de privacidade, mas também do seu léxico, passando a ser denominada privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros. Dessa forma, opera-se na

[29] RODOTÀ, Stefano. **A vida da sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.p.113

[30] DONEDA, Danilo. Da privacidade à proteção de dados pessoais, cit., p. 144-145"

[31] "Nessa perspectiva, e avaliando a trajetória da matéria nas últimas décadas, revela-se uma série de interesses a ela relacionados, não somente com respeito à reserva e ao isolamento, porém à construção de uma esfera pessoal na qual seja possível uma liberdade de escolha e, consequentemente, o desenvolvimento da personalidade. O fato de que esse interesses se encontram frequentemente em jogo quando da coleta e uso de informações pessoais impulsionou uma leitura da privacidade que, contextualizada com o conjunto de seus efeitos, foi identificada por Stefano Rodotà como a "tutela das escolhas de vida contra o controle público e a reprovação social", no quadro que ele denominara de "liberdade das escolhas existenciais". DONEDA, Danilo. Da privacidade à proteção de dados pessoais, cit., p. 144-145"

> dogmática e na prática jurídica uma clara evolução no direito à privacidade."[32]

Nesse sentido, a Corte alemã, reconheceu a autonomia dos direitos à proteção dos dados pessoais e à autodeterminação informacional, destacados do direito à privacidade[33]. O julgado alemão exemplifica que o cidadão tem capacidade de autodeterminar os seus dados, e que é um direito fundamental para desenvolver livremente sua personalidade. Contudo, a atividade de *big data* deve ter limites, estabelecendo critérios que não violem o direito da personalidade. Aponta, Bruno Ricardo Bioni:

> "(...) Esse poder [do uso de dados] necessita, sob as condições atuais e futuras do processamento automático de dados, de uma proteção especialmente intensa. Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (...) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas"[34]

Ademais, em voto na ADI 6390 DF, o Ministro Luiz Fux destaca "que a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada". Isto é, reconheceu a autodeterminação informativa como direito fundamental, ressaltando que não existem dados insignificantes no contexto atual de automatização de processos.

Deste modo, com essa garantia de que todos os dados pessoais sejam protegidos, é possível o tratamento de dados sem o consentimento do titular, no entanto, este

---

[32] MENDES, Laura, Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

[33] MARTINS, Leonardo. (org.) Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 239.

[34] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Forense, 2019, p. 132, e-book.

procedimento deve ter legalidade, e sobretudo, à luz dos princípios que a LGPD dispõe, assegurar uma finalidade determinada quando tratados.

É, portanto, admitido que as empresas desenvolvam seus estabelecimentos com o livre fluxo de dados, aliás, é um dos fundamentos das leis de proteção de dados[35], visto que é importante para o desenvolvimento econômico da sociedade, desde que respeitados a tutela jurídica de proteção de dados pessoais.

II – A LEI GERAL DE PROTEÇÃO DE DADOS

No capítulo anterior, restou demonstrado que na "Era de dados" o tratamento de dados é imprescindível para as empresas manterem sua relevância e desenvolvimento tecnológico e econômico. A sociedade de informação já é uma realidade, visto que as empresas mais valiosas do mundo contemporâneo são as empresas de tecnologia, são as empresas de dados, sendo elas: Facebook, Google, Amazon, Apple e Microsoft.

Dito isso, vimos que esse novo modelo de negócio apesar de permitir a livre circulação de dados, devem apresentar uma relação com o princípio da autodeterminação, em que os cidadãos exercerão algum controle sobre suas informações pessoais, e se utilizados, necessitam ter consentimento e finalidade.

Neste capítulo, a presente pesquisa vai abordar regulamentos e diretivas de proteção de dados, com destaque RGPD, que de certa forma influenciaram na criação da Lei Geral de Proteção de Dados no Brasil. Além disso, serão elucidados regras e princípios da lei brasileira, a serem obedecidos pelas empresas.

Outrossim, será explicado importantes instrumentos que as empresas deverão utilizar para identificar os riscos à privacidade nas atividades de tratamento de dados pessoais, e a influência, a qual o ordenamento brasileiro optou por uma proteção de dados pessoais através de um sistema de gerenciamento de riscos.

---

[35] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.26

Por fim, será analisado as responsabilidades e sanções administrativas na Lei Geral de Proteção de Dados – LGPD.

5. Regulamento Geral Proteção de Dados (RGPD) na Europa

Na década de 1970, a primeira lei direcionada a proteção de dados foi a Lei do Estado de Hessen, na Alemanha. Após, os países como França, Noruega, Suécia e Áustria implementaram formalidades para o tratamento de dados.[36] No entanto, diante o aumento de fluxo de dados e avanços tecnológicos, tornaram-se obsoletos.

Logo em seguida, por volta de 1981, a Convenção 108, foi elaborada pelos países membros do então Conselho da Europa[37], este documento concebe o primeiro tratado internacional submetendo regras sobre a proteção de dados[38], sobretudo, a sistematizar o tratamento automatizado de dados pessoais[39].

Tempos depois, o Parlamento Europeu deliberou a Diretiva 95/46/CE, esta que não mais vige, foi o texto em matéria de proteção de dados era referência até o ano de 2008. A diretiva estipulou um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais[40], mas restou ineficiente, visto os custos e ausência de sanções contra a violação das regras impostas, além disso, de acordo com Doneda[41] a prática de autodeterminação informativa foi utilizada por uma minoria da população.

---

[36] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.27

[37] O Conselho da Europa foi fundado em 1949 tendo Bélgica, Dinamarca, França, Irlanda, Itália, Luxemburgo, Países Baixos, Noruega, Suécia e Reino Unido como Estados membros, atualmente integra 47 Estados membros que ratificaram a Convenção Europeia dos Direitos do Homem. (CONSELHO DA EUROPA, 1981)

[38] "[...] internacional vinculativo que impõe algumas restrições aos fluxos transfronteiriços de dados pessoais para Estados onde a regulamentação legal não oferece proteção equivalente" (CONSELHO DA EUROPA, 1981).

[39] "além de fornecer garantias em relação à coleta e processamento de dados pessoais, [...] proíbe o processamento de dados sensíveis sobre raça, política, saúde, religião, vida sexual, antecedentes criminais, etc., na ausência de salvaguardas legais." (CONSELHO DA EUROPA, 1981)

[40] Recital 7 da Diretiva 95/46/EC.

[41] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro. 2014.p.19

Tendo em vista, que as normas e diretivas eram incompatíveis com o impacto de tratamento de dados em grandes empresas, o Parlamento, o Conselho e a Comissão da União Europeia, aprovaram uma legislação específica que padronizou regras de proteção de dados pessoais, em 27 de abril de 2016, revogando a Diretiva 95/46/EC, e intitulado de *General Data Protection Regulation* – GDPR.

Após um período de 2 anos de *vacatio legis*, o GDPR entrou em vigência em 25 de maio de 2018, para todos os Estados-membros. O GDPR, ou na forma traduzida Regulamento Geral de Proteção de Dados (RGPD), diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, ademais, a sua aplicação alcança não somente o território da União Europeia, mas também com efeitos a países terceiros, com a aplicação extraterritorial em hipóteses determinadas pela lei.

As diretrizes do Regulamento Geral de Proteção de Dados, apresentou uma perspectiva diversa da autodeterminação dos sujeitos de dados, e decidiu focar na responsabilização dos sujeitos envolvidos no processamento de dados pessoais. Nesse sentido, o legislador do regulamento europeu vai optar por uma abordagem de gerenciamento de risco[42]. Essa característica não significa que os parâmetros de direitos individuais serão ignorados, mas é uma ideia fundamentada em um balanceamento de interesses, isso quer dizer, que o processamento de dados deve servir aos funcionamentos da humanidade, não sendo o direito à privacidade absoluto. Será observado, portanto, os interesses de cada ator envolvido. Assim, dispõe na Razão 4 da RGPD:

> "Tradução livre: (4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdade e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de

[42] "Trata-se de uma opção clara pela abordagem de gerenciamento de riscos (risk-based approach), em contraposição ao modelo que privilegia a imposição de direitos (rights-based approach)" (CABRAL, Filipe Fonteles. Proteção de Dados Pessoais na Atividade Empresarial: Gerenciamento de Riscos e o Relatório de Impacto à Proteção de Dados. 2019. p.36)

> expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística." [43]

Em outros termos, a RGPD vai impor normas para o tratamento de dados pessoais realizadas no âmbito corporativo através de investigações internas, os quais vão registrar indicando os motivos pelos quais coletou e tratou os dados, apresentando a necessidade vinculada ao tratamento, a proporcionalidade das medidas aplicadas, assim como os riscos e impactos atrelados à privacidade das partes envolvidas. Esta investigação será conduzida considerando os princípios de transparência, e fundamentalmente as empresas devem observar o princípio do consentimento[44] e o legítimo interesse. Denota-se por consentimento[45] e legítimo interesse 6° e 7º do Regulamento europeu, respectivamente:

> "Art.6°: 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
>
> Art. 7º 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
> b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
> c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
> d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
> e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
> f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se

[43] Razão 4. GDPR.

[44] Razão (43): A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução. (GDPR)

> prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.
> O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrônica.
> 2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.° 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX.
> 3. O fundamento jurídico para o tratamento referido no n.o 1, alíneas c) e e), é definido: a) Pelo direito da União; ou b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito. A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.o 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.
> 4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.o, n.o 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:
> a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
> b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
> c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.o, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.o;
> d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
> e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.”

Deste modo, o consentimento é uma premissa por parte do particular, a ser realizada por um ato claro e positivo do cidadão que em toda operação de processamento ou uso de dados deve ser disponibilizado. Enquanto o legítimo interesse,

é a homologação deste processamento de informações pessoais, no qual a organização ou terceiro, tem um interesse lícito e justificado no processamento, que vai sobrepor aos direitos dos indivíduos cuja informação pessoal está sendo processada.

Em suma, essa abordagem, que mais para frente veremos que será utilizada pela legislação de proteção de dados brasileira, busca um equilíbrio de interesses dos atores envolvidos, para não afetar as ascensões tecnológicas e as atividades empresariais, bem como não ultrapassar os limites da privacidade.

A Helen Nissanbaun explica que essa regulação de proteção é a chamada de "Teoria da Integridade contextual", em que o processamento legítimo deve ser mais flexível em razão da confiança e a conformidade em alto nível de proteção de dados pessoais e aos direitos de titulares. Sendo assim, a gestão de crises das empresas vai considerar situações realísticas, para interpretar os riscos e trazer uma aplicabilidade mais efetiva da norma legal.

> Por Teoria da Integridade Contextual, Helen cita: "Temos o direito à privacidade, mas não é um direito de controlar informações pessoais, nem o direito de ter acesso a essas informações restritas. Em vez disso, é um direito de viver em um mundo no qual as expectativas que são moldadas não apenas pela força do hábito e pela convenção, mas uma confiança geral no apoio mútuo que esses fluxos concebem aos principais princípios organizadores da vida social, incluindo os morais e políticos. Esse é o direito que chamei de integridade contextual, alcançada através do equilíbrio harmonioso de regras sociais, ou normas, com valores, fins e propósitos locais e gerais"[46]

Dessa forma, a abordagem de risco utilizada pela RGPD, obriga as empresas não apenas avaliar os riscos de danos aos indivíduos, mas subsidiariamente aplicar medidas técnicas e organizativas que forem pertinentes para assegurar e comprovar que o tratamento de dados está em conformidade pelo regulamento. Ademais, o art. 4º da RGPD[47], dispõe que essas medidas devem ser constantemente revistas e atualizadas

[46] NISSEBAUM, Helen Fray. Privacy in contexto: technology, policy, and the integrity of social life. Stanford University Press, 2010. p. 231

[47] Tradução livre: art. 24: 1.Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

pelas empresas, de acordo com as suas necessidades casuistamente. Essas medidas, incluem políticas e/ou programas internos de tratamento de dados, que traz uma flexibilidade para organizações determinarem suas próprias metodologias de proteção de dados, isso porque segundo BINNS argumenta, esse método seria uma metarregulação:

> "A noção de meta-regulação, introduzida por Christine Parker, descreve sobre outras formas de regulação é que ela se apega à capacidade inerente das empresas de administrar a si mesmas, mas sem deixá-las escapar, se seus esforços de autorregulação estiverem aquém das expectativas dos reguladores (e das partes interessadas). Destina-se a alavancar as estruturas de gestão existentes das corporações e processos burocráticos internos na busca de meta regulatórias. As empresas podem ser forçadas a avaliar e relatar suas próprias estratégias de autorregulação para que as agências reguladoras possam determinar se os objetivos substantivos finais estão sendo atingidos. Os exemplos incluem segurança informacional e regulamentações alimentares que exigem que as empresas se envolvam em seus próprios processos de identificação perigos, avaliação de risco e controle de riscos. Defendo que esta abordagem, se realizada de forma adequado, tenho potencial de abordar alguns dos principais desafios e identificados pela comissão na motivação para a reforma da proteção atual." [48]

Por conseguinte, concluída essa autoanálise, o regulamento europeu na forma do art. 35º, relata que as empresas quando avaliarem dados de risco, devem fazer uma avaliação de impacto da proteção de dados, chamado pelo *Data Protection Impact Assessment* – DPIA, este documento vai ser recomendado em casos que representem um alto risco de violação à direitos e liberdades físicas.:

> "Art. 35: 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e

---

2.Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.
3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40º ou de procedimentos de certificação aprovados conforme referido no artigo 42º pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento. (GDPR)

[48] BINNSY, REUBEN. Data Protection impact assessments: a meta-regulatory approach. Internacional Data privacy Law, v.7, n.1, p 23, 2017)

finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.

3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o nº 1 é obrigatória nomeadamente em caso de:

a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9° n°1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; ou

c) Controlo sistemático de zonas acessíveis ao público em grande escala.

4. A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do nº 1. A autoridade de controlo comunica essas listas ao Comité referido no artigo 68º.

5. A autoridade de controle pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados. A autoridade de controlo comunica essas listas ao Comité.

6. Antes de adotar as listas a que se referem os n.º 4 e 5, a autoridade de controlo competente aplica o procedimento de controlo da coerência referido no artigo 63.o sempre que essas listas enunciem atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controlo do seu comportamento em diversos Estados-Membros, ou possam afetar substancialmente a livre circulação de dados pessoais na União.

7. A avaliação inclui, pelo menos:

a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n° 1; e

d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

8. Ao avaliar o impacto das operações de tratamento efetuadas pelos responsáveis pelo tratamento ou pelos subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, é tido na devida conta o cumprimento dos códigos de conduta aprovados a que se refere o artigo 40.o por parte desses responsáveis ou subcontratantes.

9. Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento.

10. Se o tratamento efetuado por força do artigo 6.o, n° 1, alínea c) ou e), tiver por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico, não são aplicáveis os nº 1 a 7, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento.

11. Se necessário, o responsável pelo tratamento procede a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo menos quando haja uma alteração

> dos riscos que as operações de tratamento representam."[49] Tradução livre, GDPR.

O procedimento de DPIA, é moldado da seguinte maneira, exemplificando o disposto no artigo acima. Em obediência ao princípio da responsabilidade (art. 5°, da RGPD), o relatório deve conter[50]:

- **Descrição do processamento e dos propósitos;**
- **Interesses legítimos prosseguidos pelo controlador;**
- **Avaliação da necessidade e da proporcionalidade do processamento;**
- **Avaliação dos riscos para os direitos e liberdades dos titulares dos dados;**
- **Medidas previstas para abordar os riscos;**
- **Salvaguardas e medidas de segurança para demonstração da conformidade;**
- **Indicação de qualquer proteção de dados by design e by default;**
- **Lista de destinatários de dados pessoais;**
- **Confirmação da conformidade com os respectivos códigos de conduta aprovados;**

Dito isto, esses são alguns dos pontos do RGPD, que inspirou a legislação brasileira de proteção de dados. Portanto, no próximo tópico, será abordado os principais pontos do regulamento brasileiro de proteção de dados, além de tratar a abordagem de gerenciamento de risco, e desta maneira, comentar sobre o documento de Relatório de Impacto à Proteção de Dados – RIPD.

6. A Lei Geral de Proteção de Dados Pessoais – LGPD: princípios e abordagem de gerenciamento de risco.

[49] GDPR, art. 35.
[50] Disponível em: https://www.certifiquei.com.br/dpia/ (acesso em 19/09/2021)

No cenário brasileiro, a Lei Geral de Proteção de Dados Pessoais, foi criada não exclusivamente inspirada na RGPD para normatizar a proteção e privacidade de dados, mas também encontrou uma inspiração em outras normas do ordenamento, como na Constituição Federal (Art.5º, X e LXXVII) e o Marco Civil da Internet (Lei nº 12.595/14), e outros dispositivos esparsos.

Na verdade, pode-se dizer que a LGPD foi elaborada analisando as questões discutidas pela RGPD, e apresentou seus textos mais orientativos no bojo da realidade brasileira. Dessa maneira, o estudo do presente tópico vai correlacionar aspectos do regulamento europeu, bem como, esclarecerá os princípios e o texto da legislação brasileira.

6.1 Aspectos Gerais

É inegável que o Regulamento europeu de proteção de dados foi um marco ao tratar a privacidade e tutela jurídica dos dados. Seus princípios e regras obtiveram uma repercussão global, isso porque dentre outros motivos, determinou efeitos extraterritoriais[51] aos controladores e processadores de dados. Nesse sentido, além de buscar uma maior proteção de dados aos titulares, consequentemente facilita as transações comerciais e a cooperação entre as organizações e autoridades públicas[52].

---

[51] Art.27, GDPR: "**1.** Se for aplicável o artigo 3°, n.2, o responsável pelo tratamento ou o subcontratante designa por escrito um representante seu na União.
2. A obrigação a que se refere o n. 1 do presente artigo não se aplica:
a) Às operações de tratamento que sejam ocasionais, não abranjam o tratamento, em grande escala, de categorias especiais de dados a que se refere o artigo 9.o, n. 1, ou o tratamento de dados pessoais relativos a condenações penais e infrações referido no artigo 10.o, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento; ou
b) Às autoridades ou organismos públicos;
3. O representante deve estar estabelecido num dos Estados-Membros onde se encontram os titulares dos dados cujos dados pessoais são objeto do tratamento no contexto da oferta que lhes é feita de bens ou serviços ou cujo comportamento é controlado.
4. Para efeitos do cumprimento do presente regulamento, o representante é mandatado pelo responsável pelo tratamento ou pelo subcontratante para ser contactado em complemento ou em substituição do responsável pelo tratamento ou do subcontratante, em especial por autoridades de controlo e por titulares, relativamente a todas as questões relacionadas com o tratamento.
5. A designação de um representante pelo responsável pelo tratamento ou pelo subcontratante não prejudica as ações judiciais que possam vir a ser intentadas contra o próprio responsável pelo tratamento ou o próprio subcontratante."

[52] A tutela dos dados online e a preservação da privacidade têm se revelado bastante problemáticas porque a extraterritorialidade da rede oferece amplas possibilidades de descumprimento das normativas e levanta o questionamento do conflito entre as diferentes legislações dos países. É inegável que o fluxo de

Nesse aspecto, visando melhores práticas no fluxo de dados e fortemente inspirada pela RGPD, a Lei Geral de Proteção de Dados Pessoais é sancionada em agosto de 2018, entrando em vigor em agosto de 2020.

Em suma, a lei objetiva a proteção de direitos e garantias fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania por pessoais naturais (art. 1°, LGPD).

Assim sendo, a LGPD trata de todas as operações realizadas com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;[53]

Neste seguimento, de acordo com o art. 5° da LGPD, há dois personagens de notoriedade para o tratamento de dados, o "controlador", que será a pessoa física ou jurídica a quem compete a decisão sobre o tratamento do dado, e o "operador", será aquele que realiza o tratamento de dados em prol do controlador. Ambos são agentes de tratamento de dados, no entanto apesar de a tomada de decisão quanto ao tratamento de dados ocorra sobre a responsabilidade do controlador, o operador não se desobriga de tratá-los em estrita observância à boa-fé e aos princípios de proteção de dados consolidados no art.6°.

---

dados transfronteiras tem provocado a preocupação das grandes organizações internacionais" (PAESANI, Liliana Minardi. Garantia Fundamental do não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei. In: LEITE, George Salomão; LEMOS, Ronaldo Lemos (Coord.). Marco Civil da Internet, São Paulo: Atlas,2014. p.523).

[53] 5°, X, da LGPD - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Ademais, ressalta-se, que a LGPD, fixa deveres aos agentes de tratamento no tocante ao comprometimento à adoção de regras de governança[54], assim como a criação de um departamento ou nomear um Encarregado de Proteção de Dados (*Data Protection Officer* – DPO) (art. 41), sob pena das empresas sofrerem sanções previstas no art. 52, LGPD.

Todavia, para compreender os requisitos deste programa estrutural de governança, é fundamental estudar os princípios e objetivos que estabeleceu a legislação brasileira de proteção de dados pessoais.

6.2 Fundamentos e Princípios

[54] Art. 50, da LGPD: " Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
I - implementar programa de governança em privacidade que, no mínimo:
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Conforme exposto anteriormente, e extraído do art.1° da LGPD, o objetivo desta lei é a proteção de direitos e garantias fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania por pessoais naturais.

Outrossim, estabelece que os fundamentos desta lei, nos termos do art. 2°, é assegurar a pessoa natural a titularidade de o controle sobre informações pessoais amparadas de proteção legal, respaldando-se no respeito à privacidade, na autodeterminação informativa, no desenvolvimento econômico e tecnológico, bem como na livre-iniciativa, livre concorrência e a defesa do consumidor.

A partir disso, destaca-se que a privacidade recebe o *"status"* tanto de objetivo, quanto de fundamento. Isso significa que no rol de fundamentos, a privacidade é igualmente importante aos preceitos do desenvolvimento econômico. Ou seja, nas palavras de Filipe Fonteles:

> "embora prescreva um fim a ser alcançado (proteção a direitos fundamentais), tal objetivo não pode afastar alicerces maiores (fundamentos da disciplina). Em outras palavras, a regulação da LGPD busca a proteção da privacidade, dede que tal proteção não seja desproporcional ou impeditiva da inovação, já que a privacidade e o desenvolvimento econômico são valores de igual patamar neste contexto legislativo"[55]

Dessa forma, a LGPD vai dispor no art. 6°, dez princípios norteadores da proteção de dados pessoais, que deverão observar a boa-fé. Para o presente estudo, a fim de elucidar a abordagem de gerenciamento de risco, serão estudados os princípios da finalidade, adequação, necessidade, transparência, segurança e responsabilização.

6.2.1: Princípio da Finalidade

"Art. 6º, inciso I: finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;"

[55] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.56

O princípio da finalidade determina o tratamento de dados deve ter uma finalidade especificada e informada explicitamente ao titular. No mais, o tratamento de dados deve ser utilizado com cautela pelo controlador, uma vez que deve ser delimitado os propósitos almejados que servirão para o uso de dados pessoais. É importante que as partes envolvidas tenham um comum entendimento do objetivo do tratamento.

Diante disso, o controlador deve se atentar para que após o cumprimento da finalidade delimitada não haverá mais necessidade do uso dos dados coletados uma vez que LGPD determina o término do tratamento dos dados pessoais com a sua posterior eliminação, sendo autorizada a sua conservação apenas em hipóteses específicas.[56]

6.2.2 Princípio da Adequação

"Art. 6º, inciso II adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;"

O princípio da adequação conforme texto normativo, tem a sua interpretação atrelada ao princípio da finalidade. Em razão disso, informado ao titular os fins de uso dos dados, estas devem ser compatíveis como o que for consentido, no contexto do tratamento.

6.2.3 Princípio da Necessidade

"*Art. 6º, inciso III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;'*

O princípio da necessidade determina que o tratamento de dados será limitado ao mínimo necessário para realização da sua finalidade. Dessa forma, cabe destacar que o controlador vai utilizar a ponderação acerca da real necessidade de coleta de uso de dados pessoais para finalidade desejada, e nos casos em que o objetivo seja alcançado

[56] PIRONTI, Rodrigo. Lei Geral de Proteção de Dados: Estudos sobre um novo cenário de governança corporativa. Belo Horizonte. Ed: Forum. 2020. p.182.

através de outro meio sem a utilização de dados pessoais, o controlador deve sobrepor esse método.[57]

Nesse sentido, afasta a coleta de dados pessoais supérfluos para determinada finalidade, e diminui os riscos de invasão desproporcional à privacidade do titular.

6.2.4 Princípio da Transparência

"Art. 6°, inciso VI: Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;"

O princípio da transparência garante aos titulares de dados o acesso simplificado e compreensível das informações acerca do tratamento de dados e os agentes que integram essa cadeia. No entanto, a LGPD de forma expressa limita o direito dos titulares de dados a transparência quando houver conflito com os segredos de negócios contidos nos processos ou algoritmos do controlador, em razão do direito de propriedade intelectual das empresas.

O princípio da ponderação deve ser invocado nesses casos, visto que este procedimento está atrelado em gerar confiança ao titular sobre seus direitos e as tomadas de decisão feitas pelo controlador. Assim como, não sobrepor nenhum direito aos segredos de negócios do controlador.

6.2.5 Princípio da Segurança

"Art. 6º, inciso VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;"

---

[57] VAINZ, Rony. Disposições Preliminares, *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). LGPD – Lei Geral de Proteção de Dados comentada. São Paulo: Thompson Reuters Brasil, 2019. P.144.

O princípio da segurança está vinculado as políticas de integridade que são implementadas pelas empresas. Ressalta-se, que as medidas que o texto normativo dispõe, faz parte de deveres que os agentes de tratamento adotem políticas de boas práticas e governança no tratamento de dados pessoais, conforme artigo 50 da LGPD, ao afirmar que essas medidas vão além de segurança digital.

Na verdade, o propósito desse princípio é que as regras de integridade das empresas reflitam na organização, documentação, publicação e implementação de política de privacidade do controlador e operador. Os controles internos dos agentes de tratamento de dados, exigidos pela LGPD, vão exprimir a exposição ao risco e a violação à privacidade, por isso seu comprometimento com medidas de controle e prevenção de segurança de informações devem ser priorizados. [58]

Inclusive, o art. 44, parágrafo único da LGPD, determina expressamente a responsabilidade pelos danos decorrentes da violação de segurança dos dados aos agentes que não adotarem as medidas de segurança adequadas.

Nesse aspecto, é factível que a abordagem de avaliação de risco adotada pela legislação é essencial para evitar esse ônus aos agentes de tratamento.

6.2.6 Princípio da Responsabilização

"Art. 6º, inciso X: responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

O princípio da responsabilização e prestação de contas demonstra expressamente que as empresas, e, portanto, os agentes de tratamento de dados, devem adotar medidas de segurança e governança, comprovando-se a eficácia e efetividade para o cumprimento dos objetivos desta lei.

---

[58] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.64-65

De acordo com o art. 42 da LGPD, essa responsabilização se estende aos seus fornecedores e terceiros que atuem como operadores de dados. Nesse sentido, informa que a responsabilidade é solidária e reduz o fardo dos titulares nos casos de vazamentos de dados, aumenta a demanda dos controladores.

Desse modo, interpreta-se a responsabilização com repercussão direta na abordagem de gerenciamento de risco. Com isso, as empresas com a devida proporcionalidade, vai arrazoar seus interesses em conformidade com os princípios e fundamentos da lei de proteção de dados.

6.3 Abordagem de gerenciamento de risco da LGPD

A percepção de autorregulação no Regulamento europeu discutida anteriormente, em síntese aduziu que essa abordagem estratégica para o tratamento de dados, estimula as empresas adotarem boas práticas de governança na coleta e uso de dados pessoais, e reguladas por sanção em caso de descumprimento. Nesse sentido, a legislação brasileira adota a abordagem de gerenciamento de risco de forma mais ampla e flexível que a RGPD, que cataloga seis bases legais para o tratamento de dados: o consentimento explícito, desempenho contratual, tarefa pública, interesse vital, obrigação legal e interesse legítimo. Enquanto a LGPD, na forma do art. 7°, elenca dez requisitos, acrescentando mais quatro hipóteses: os estudos de um órgão de pesquisa, exercício de direitos em processos judiciais, proteção à saúde e proteção ao crédito:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.[59]

De forma exemplificada, o tratamento de dados poderá ser realizado para o cumprimento de obrigação legal ou regulatória nos seguintes casos:

a) Consentimento: O titular de dados autoriza o uso dos seus dados para uma ou mais finalidades, que devem ser claras e objetivas.

Infere-se por titular à pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Por consentimento o art. 5°, da LGPD, define "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"

b) Cumprimento de obrigação legal: O tratamento de dados é realizado para cumprimento de imposições legais, tal medida reduz conflitos com demais leis do ordenamento.

c) Execução de políticas públicas: Na Administração Pública, o tratamento de dados é executado, exclusivamente, para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou de repressão às infrações legais.

d) Estudos por órgão de pesquisa: O tratamento de dados é utilizado para realização de estudos por órgãos de pesquisa, e sempre que necessário, anonimizando os dados pessoais ao que se refere.

[59] Lei Geral de Proteção de Dados Pessoais.

e) **Execução de Contrato/ diligências pré-contratuais:** O tratamento de dados assegura a execução de um contrato ou de seus procedimentos preliminares. Nesse sentido, o titular de dados não poderá revogar o seu fornecimento a qualquer momento, em razão da outra parte ter seu direito resguardado pela LGPD para manter os dados fornecidos pelo durante a vigência do contrato em que foi acordado.

f) **Exercício regular de direitos:** O tratamento de dados garante o exercício regular de direitos em processos judiciais, administrativos ou arbitrais.

g) **Proteção à vida:** A finalidade deste tratamento de dados, é no intuito de proteger a vida ou a incolumidade física do titular ou terceiro.

h) **Tutela de saúde:** O tratamento de dados deve ser realizado por profissionais de saúde, serviços de saúde ou autoridades sanitárias, com a finalidade de tutela de saúde.

i) **Interesses legítimos do controlador/terceiro:** O tratamento de dados é realizado para atender os interesses legítimos do controlador ou terceiro, desde que não ofereça riscos aos direitos e liberdades fundamentais do titular de dados pessoais,

j) **Proteção de Crédito:** Quando os titulares de dados pessoais ao contrair dívidas, e tentar se beneficiar com a lei para evitar a cobrança, o tratamento de dados é vai ser permitido para evitar brecha legislativa e o não pagamento dessas dívidas.

Dessa forma, a LGPD estabelece que o primeiro requisito legal para o processo de tratamento de dados, é determinando uma finalidade específica, de acordo com rol apresentado pelo art. 7°. No entanto, a lei adiciona mais duas condições especiais para o tratamento: de dados pessoais sensíveis (cf. arts. 11, 12 e 13) e os dados pessoais de titularidade de crianças ou adolescentes (cf. art.14).

Por conseguinte, o controlador deve fundamentar-se no legítimo interesse previsto no art. 10°:

> "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e

> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

As disposições do artigo 10, aponta no §1°, que o tratamento desses dados deverá ser manuseado apenas quando estritamente necessários e vinculados com a finalidade outrora determinada.

Além disso, estabelece no seu § 2° que obrigatoriamente deverá ser feito um mapeamento de quais dados serão coletados e tratados ao longo do processo. Em seguida, as empresas deverão adotar medidas de transparência, sendo recomendado a elaboração do Relatório de Impacto à Proteção de Dados Pessoais – RIPD, (cf. art. 5°, XVII, LGPD), esta que poderá ser solicitada pela Autoridade Nacional de Proteção de Dados (cf. Art.10, §3°).

Em suma, a lei aponta que a adoção dessas boas práticas equilibra os interesses das partes envolvidas, considerando, quando falamos dos fundamentos desta lei, a privacidade e o desenvolvimento de tecnologia e inovação são igualmente importantes.

Para concluir o presente estudo, entendendo os preceitos da LGPD, e o seu contexto, será abordado no próximo tópico sobre a RIPD, bem como instruções de boas práticas necessárias para as empresas se adequarem;

III – Requisitos impostos pela LGPD para adequação das empresas

Apresentou-se ao longo do capítulo anterior que a LGPD optou por um sistema de gerenciamento de risco, os quais deverão ser implementados políticas de governança para evitar possíveis aplicações de sanções às empresas.

Essas medidas estão relacionadas à instrumentos para identificar riscos em atividades de tratamento de dados, de modo que não haja qualquer violação a direitos dos titulares de dados pessoais.

Por isso, a legislação indica a elaboração do relatório com um foco investigativo, o mencionado Relatório de Impacto à Proteção de Dados (RIPD), será essencial para formalizar os riscos e impactos relacionados ao tratamento de dados pessoais, sobretudo para assegurar os princípios da LGPD, com destaque para o princípio da responsabilização.

Ademais, será abordado algumas práticas internas importantes na condução desses procedimentos nas empresas, principalmente porque além do cumprimento de preceitos legais de proteção de dados, é primordial a confiança dos clientes e colaboradores, a fim de evitar vazamentos, firmando-se a segurança jurídica dos dados.

7. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais, conforme abordado no tópico 5 foi inspirado na RGPD, que descreve no art. 35, os procedimentos necessários para elaboração do relatório de avaliação de risco.

Na LGPD, esse instituto recebeu o nome de RIPD, positivada no art. 5°, XVII, que define:

> "Art. 5º Para os fins desta Lei, considera-se:
>
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;"[60]

De acordo com o descrito, o controlador vai produzir essa documentação, analisando e mitigando os possíveis riscos no tratamento de dados. No art. 38, caput, da LGPD, de outro modo, o legislador delega à ANPD a regulação do conteúdo de RIPD,

[60] Lei Geral de Proteção de Dados

bem como descreve no parágrafo único, os requisitos mínimos para a elaboração do relatório.

> "Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."

Dessa forma, o art. Art.10, § 3°, ressalta que a ANPD, tem o direito de solicitar às empresas o relatório de impacto à proteção de dados. Portanto, visto que tal documentação pode ser exigida, vincula as empresas à adoção dessa medida. Sendo assim, combinando os artigos supracitados, destaca-se os requisitos mínimos do RIPD[61]:

- Descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais;
- Medidas, salvaguardas e mecanismos de mitigação de risco;
- Avaliação de interesse legítimo (nas hipóteses que a lei determina);
- Descrição dos tipos de dados;
- Metodologia utilizada para obtenção de dados;
- Metodologia utilizada para garantia da segurança de informações;
- Análise do controlador com relação as medidas, salvaguardas e mecanismos de mitigação de risco.

Ressalta-se também, que esse relatório deve ser produzido pelo controlador antes de iniciado o tratamento de dados, essa ação é primordial para a prevenção e segurança a tutela de proteção desses dados.

---

[61] CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019, p.99

Para melhores decisões e conselhos no RIPD, a lei determina a nomeação de um Encarregado (Art. 23 c/c Art. 39, da LGPD[62]), o qual conhece a fundo a legislação e seus objetivos, denominado de Encarregado de Proteção de Dados, ou DPO (*Data Protection Officer*). O art. 5°, VIII, define o encarregado:

> "VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

O Encarregado pela sua experiência e expertise na matéria, orientará a empresa sobre as ações que devem ser tomadas para adequação à Lei. Nesse sentido, as atividades do encarregado, são apresentadas pelo Art. 41, da LGPD:

> "Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
>
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
>
> § 2º As atividades do encarregado consistem em:
>
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
>
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados."

---

[62] Lei de Proteção de Dados "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;
Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria."

Logo, o Relatório de Impacto à Proteção de Dados, objetiva medidas de transparência e de responsabilização do controlador, é uma ferramenta que elucidará no gerenciamento de riscos, bem como para demonstrar a sua conformidade com os fundamentos e princípios da lei. É também uma medida protetivas para que as empresas evitem sanções e ações judiciais.

Além dos requisitos mínimos trazidos anteriormente, é importante atentar-se para alguns passos para elaboração da RIPD:

a) identificar quem são os agentes de tratamento;

b) nomear o Encarregado de Proteção de Dados;

c) descrever os tipos de tratamentos de dados pessoais que serão realizados;

e) verificar as partes interessadas para elaboração do relatório;

f) determinar e qualificar todos os possíveis riscos para os tratamentos de dados;

g) especificar diferentes medidas que serão utilizadas para agir sobre os riscos;

h) validar o relatório com a aprovação de um Encarregado de Proteção de Dados; e por fim,

i) manter uma revisão constante sobre o documento;

8. Responsabilidades e sanções administrativas na LGPD

Até então, no presente estudo, foram abordados pressupostos para compreensão da necessidade de autorregulação das empresas no tratamento de dados. Comentou-se alguns requisitos mínimos que as empresas devem observar para não ultrapassar os limites de privacidade dos titulares, a fim de que não sofra sanções administrativas. Neste tópico, será abordado brevemente as espécies de sanções e a responsabilidade dos agentes de tratamento de dados.

No bojo do art. 52, a LGPD, prevê que a ANPD aplicará sanções administrativas aos agentes de tratamento que infringirem à lei.

Dessa maneira, A Lei Geral de Proteção de Dados, na forma do artigo 55-A[63], estabeleceu ANPD como órgão da Administração Pública Federal. À vista disso, é possível identificar três funções deste órgão: consultivo, regulador e sancionador, que deverão ser exercidas por meio de uma autonomia técnica e decisória.

No âmbito da sanção administrativa para configurar uma infração é necessária a configuração de conduta contrária aos ditames da lei, nesse cenário é realizado um processo de apuração. Na LGPD, a ANPD assim que identificar um comportamento, ou seja, ação ou omissão praticada pelo agente de tratamento de dados, vai iniciar a apuração da infração administrativa.

A primeira sanção que o artigo 52, I, da LGPD traz, é a advertência, a ANPD com medidas corretivas diante de uma infração mais leve, indicando um prazo correção, levando em consideração à proporcionalidade.

No, incisos II e III do art. 52, a lei prevê multa simples e diária, sendo a multa simples de 2% do faturamento da empresa, limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, e a multa diária recai sobre o mesmo limite total.

No inciso IV, temos a sanção de publicização da infração, após devidamente apurada, com a publicação da decisão condenatória, decorre de ampla divulgação nos meios de comunicação para atingir a imagem do agente de tratamento publicamente. Já as sanções previstas nos incisos V, VI e VII, trata-se de infração na própria atividade de tratamento, através de eliminação ou bloqueio dos dados até a regularização.

---

[63] Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)
§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019)
§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019)
§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.

Em seguida, o inciso X prevê a suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador. Nesse caso, o prazo permanece até a regularização, ainda que antes do prazo de seis meses, entretanto, persistindo a irregularidade, a suspensão deverá ser mantida. No inciso XI, a suspensão vai ser aplicada nos moldes no caso anterior, mas atingindo toda a atividade de tratamento a que se refere a irregularidade, e não somente o banco de dados.

Ao final, o inciso X, prevê a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, essa é considerada uma sanção mais gravosa, tendo em vista que não há um prazo especificado dessa proibição. Dessa forma, o prazo para essa penalidade, vai caber à ANPD estabelecer e motivar, com a devida proporcionalidade.

Nos casos de sanções de suspensão e proibição, conforme o art. 52, § 6°, a medida sancionatória só poderá ser aplicada após adotadas uma das demais medidas de sanções que o artigo prevê.

Ressalta-se que todo procedimento de infração, serão assegurados a ampla defesa, garantindo o devido processo legal, bem como direito à produção de provas. O § 1°, do art. 52, aduz ainda, que as sanções devem ser aplicadas de forma gradativa, isolada, ou cumulativamente, observando, motivadamente, o caso concreto e considerados os seguintes parâmetros e critérios:

> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Sobre a responsabilidade civil dos agentes, denota-se dos seguintes preceitos, primeiro de uma conduta (ação ou omissão) do controlador ou operador dos dados. Após, a configuração de dano, sendo devidamente comprovado. E por fim, o preceito de nexo causal, entre o dano causado ao titular de dados, e se responsabilização da conduta do agente de tratamento.

Outrossim, o art. 42, da LGPD, assegura aos titulares a reparação de danos materiais e morais, sendo individuais ou coletivos:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

O inciso I, do artigo supramencionado, determina, ainda, que o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, equiparando-se ao controlador. Em relação a responsabilidade aos danos por descumprir a lei, não há dúvidas, no entanto, na hipótese em que o operador não segue às instruções lícitas do controlador, a lei não é muito clara. Visto que, sendo as instruções lícitas e, portanto, em conformidade com a lei, não haveria motivo para responsabilizar o controlador.

Nesse sentido, para Marcos Gomes Silva Bruno:

> "Referido inciso equipara o operador ao controlador, quando este deixa de observar as instruções lícitas do controlador. Vale dizer, se a empresa

> contrata um terceiro para operar dados pessoais e ele trata aqueles dados em desacordo com a orientação do controlador, inicia uma nova atividade de controle do dado, estranha a atividade que lhe foi delegada. De acordo com as circunstâncias, essa pode ser a hipótese de exclusão de responsabilidade do controlador, como, aliás, é expressamente previsto no artigo 43 da lei geral de proteção de dados." [64]

Por fim, o artigo 43 da LGPD preceitua sobre as excludentes de responsabilidades, cenário no qual, os agentes de tratamento não serão responsabilizados, mediante comprovação. Em síntese, prevê três excludentes: a primeira é em relação conduta, nos casos em que não há sequer conduta atribuída ao controlador ou ao operador, dessa forma, o tratamento pode não ter sido realizado ou foi realizado por outro agente de tratamento. Na segunda hipótese, existe uma conduta do agente de tratamento, entretanto, é uma conduta lícita, sem qualquer violação a legislação. A terceira e última, exclui a responsabilidade do controlador o operador, caso dano seja por culpa exclusiva do titular de dados ou de terceiros.

[64] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). LGPD – Lei Geral de Proteção de Dados comentada. São Paulo: Thompson Reuters Brasil, 2019.

CONCLUSÃO

Em face do exposto, demonstra-se que as atividades de tratamento de dados, são essenciais para o desenvolvimento econômico, político, inovador e nos demais setores em que a análise de dados, e descobertas de padrões promova algum efeito na sociedade, e que mesmo com o eventual risco à privacidade, não são ilegais. No entanto, a ilegalidade se configura com a inadequação das empresas aos requisitos e medidas de seguranças para mitigar os riscos no tratamento desses dados.

A legislação brasileira de proteção de dados, condiciona o tratamento de dados fundamentada em dez bases legais. Ademais, determina deveres que os agentes de tratamento (controlador, operador e encarregado) devem cumprir, e constantemente revisar as medidas adotadas no processamento dos dados.

Com relação a isso, a LGPD vai estabelecer uma medida fiscalizatória, com intuito de inspirar boas práticas de governança, bem como uma autorregulação dos riscos das empresas, através do Relatório de Impacto de Proteção de Dados. Este relatório, é sobretudo, um instrumento que as empresas vão fundamentar todo e qualquer tratamento de dados pessoais, de modo que os agentes de tratamento, principalmente o encarregado, personalizarão, de maneira mais aprofundada, todas as especificidades, peculiaridades e problemas do tratamento de dados naquela empresa.

Além disso, os agentes responsáveis pelo tratamento de dados da empresa devem considerar que para mitigar os riscos do tratamento, é primordial conduzir essa adequação à LGPD com a visão empresarial, uma vez que somente entendendo as realidades particulares de cada negócio a adequação se realizará. Melhor dizendo, não há como desvencilhar o tratamento de dados realizado por empresa, sem de fato entender a atividade empresarial inerente à atividade de tratamentos de dados pessoais.

Por fim, a adequação de uma empresa aplicando medidas primorosamente organizadas e bem desenvolvidas, além de salvaguardar às empresas de medidas sancionatórias, e de multas, consistirá na confiabilidade no mercado para segurança de informação de dados, promovendo o pleno gozo da função social da empresa.

REFERÊNCIAS

BARBOSA, Pedro Marcos Nunes. *E-stabelecimento*: Teoria do estabelecimento comercial na Internet, aplicativos, websites, segregação patrimonial, , trade dress eletrônico, concorrência online, ativos inatingíveis cibernéticos e negócios jurídicos. São Paulo: Quartier Latin, 2017.p.43

BINNSY, REUBEN. Data Protection impact assessments: a meta-regulatory approach. Internacional Data privacy Law, v.7, n.1, p 23, 2017)

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Forense, 2019, p. 132, e-book.

BLUM, Renato Opice (Coord.). LGPD – Lei Geral de Proteção de Dados comentada. São Paulo: Thompson Reuters Brasil, 2019. P.144.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm, Acesso em: 21 de set. de 2021

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015 2018/2018/lei/l13709.htm, Acesso em: 21 de set. de 2021.

BRASIL. Lei n° 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm . Acesso em: 21 de set. de 2021

CABRAL, Filipe Fonteles. Proteção de Dados pessoais na atividade empresarial: gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019.

COELHO, Fabio Ulhoa. Curso de Direito Comercial, volume 1: direito de empresa. 20. ed. São Paulo: Editora: Revistas dos Tribunais, 2016, p.76

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro. 2014.p.19

DONEDA, Danilo. Da privacidade à proteção de dados pessoais, Revista dos Tribunais. 2019, cit., p. 144-145.

FÁVERO, Luiz Paulo. KDD e Data Mining: mais do que apenas conceitos. Disponível em: https://itforum.com.br/coluna/kdd-e-data-mining-mais-do-que-apenas-conceitos/. Acesso em 21/09/2021.

FIGURA, 1: Disponível em: https://www.itforum365.com.br/wp-content/uploads/2019/04/Figura-KDD-e-Data-Mining.png Acesso em 23/09/2021

FORCES, Sales. Disponível em: https://www.salesforce.com/br/crm/#crm-definicao-e-conceitos-scroll-tab. Acesso em: 19 de set. de 2021.

FRAZÃO, Ana. Plataformas digitais e os desafios para a regulação jurídica. v.1. Belo Horizonte: Editora D'Plácido, 2018.

GENERAL DATA PROTECTION REGULATION. Disponível em: https://www.privacy-regulation.eu/pt/index.htm. Acesso em: 21 de set. de 2021.

LAROSE, D. T. Discovering Knowledge in Data: An Introduction to Data Mining. John Wiley and Sons, Inc, 2005

LAUDON, Kenneth; LAUDON, Jane. Sistemas de Informações Gerenciais. 9.ed. Tradução de Luciana do Amaram Teixeira. São Paulo: Pearson Prentice Hall, 2010.p.159

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). LGPD – Lei Geral de Proteção de Dados comentada. São Paulo: Thompson Reuters Brasil, 2019.

MARTINS, Leonardo. (org.) Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão. Montevidéu: Fundação Konrad Adenauer, 2005, p. 239.

MAYER-SCHONBERGER, Viktor; CUJIER, Kenneth. Big Data: Como extrair volume, variedade e valor da avalanche de informação cotidiana. Tradução de Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013. p.70.

MENDES, Laura, Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MICKENSEY&COMPANY. Big Data, Analytics, and the Future of Marketing Sales. New York: McKinsey&Company, 2013.

NISSEBAUM, Helen Fray. Privacy in contexto: technology, policy, and the integrity of social life. Stanford University Press, 2010. p. 231

PIRONTI, Rodrigo. Lei Geral de Proteção de Dados: Estudos sobre um novo cenário de governança corporativa. Belo Horizonte. Ed: Forum. 2020. p.182.

SCHWAB, Klaus. A Quarta Revolução Industrial. Rio de Janeiro: EDIPRO, 2019.

SOARES, Fábio Lopes. Governança cidadã: alternativa para garantia da realização da função social das empresas e de sustentabilidade econômica. Revista da Faculdade de Direito de São Bernardo do Campo, São Bernardo do Campo, v. 22, n. 1, p. 1-16, 2016

VAINZ, Rony. Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Lei Geral de Proteção de Dados Comentada. 2. ed. rev., atual e ampl. São Paulo: Thomson Reuters Brasil, 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard Law Review, Vol. 4, Nº. 5. 1890, p. 193-220.

ZEFERINO, Denis. Disponível em: https://www.certifiquei.com.br/dpia/. Acesso em 21 de set. de 2021