UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE GRADUAÇÃO EM DIREITO

JOHANN BIELEMANN CUNHA

LEGÍTIMO INTERESSE: A CARTA (NADA) BRANCA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

FLORIANÓPOLIS
2021

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE GRADUAÇÃO EM DIREITO

LEGÍTIMO INTERESSE: A CARTA (NADA) BRANCA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Santa Catarina, como requisito para a obtenção do título de Bacharel em Direito.

Orientadora: Prof.ª. Dra. Liz Beatriz Sass

FLORIANÓPOLIS
2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Cunha, Johann
Legítimo Interesse: A carta (nada) branca da Lei Geral de Proteção de Dados (LGPD) / Johann Cunha ; orientadora, Liz Beatriz Sass, 2021.
64 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Graduação em Direito, Florianópolis, 2021.

Inclui referências.

1. Direito. 2. Dados Pessoais. 3. Legítimo Interesse. 4. LGPD. I. Sass, Liz Beatriz. II. Universidade Federal de Santa Catarina. Graduação em Direito. III. Título.

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COORDENADORIA DE MONOGRAFIA

ATA DE SESSÃO DE DEFESA DE TCC (VIRTUAL)

(Autorizada pela Portaria 002/2020/PROGRAD)

Aos 24 dias do mês de setembro do ano de 2021, às 14 horas e 00 minutos, foi realizada a defesa pública do Trabalho de Conclusão de Curso (TCC), no modo virtual, através do link: "https://teams.microsoft.com/l/meetup-join/19%3ameeting_ZDc0ZDZhMjEtMmVjNi00MDk5LWFlMjUtMzQ1YjliYzViNTlm%40thread.v2/0?context=%7b%22Tid%22%3a%2224139d14-c62c-4c47-8bdd-ce71ea1d50cf%22%2c%22Oid%22%3a%22aa0e18b8-ce46-47c2-aec4-7611bc083759%22%7d" intitulado **"Legítimo Interesse: A carta (nada) branca da Lei Geral de Proteção de Dados (LGPD)" ,** elaborado pelo(a) acadêmico(a) **Johann Bielemann Cunha**, matrícula **nº 16201007**, composta pelos membros **Dra. Liz Beatriz Sass, Me. Rafael M. Popini Vaz e Caio Eduardo de Souza Dias**, abaixo assinados, obteve a aprovação com nota _____(_____), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

( ) Aprovação Integral
( ) Aprovação Condicionada aos seguintes reparos, sob fiscalização do Prof. Orientador

Florianópolis, 24 de setembro de 2021.

_____
Liz Beatriz Sass
Professor Orientador

_____
Rafael M. Popini Vaz
Membro da Banca

_____
Carlos Eduardo de Souza Dias
Membro da Banca

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS JURÍDICAS

COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado "**Legítimo Interesse: A carta (nada) branca da Lei Geral de Proteção de Dados (LGPD)**"**,** elaborado pelo(a) acadêmico(a) "**Johann Bielemann Cunha"**, defendido em **24/09/2021** e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota **_____(_____)**, cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 24 de setembro de 2021

_____

Liz Beatriz Sass
Professor Orientador

_____

Rafael M. Popini Vaz
Membro de Banca

_____

Carlos Eduardo de Souza Dias
Membro de Banca

Universidade Federal de Santa Catarina

Centro de Ciências Jurídicas

COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E ORIENTAÇÃO IDEOLÓGICA

Aluno(a): Johann Bielemann Cunha
RG: 5595864 SSP/SC
CPF: 026.852.960-42
Matrícula: 16201007
Título do TCC: Legítimo Interesse: A carta (nada) branca da Lei Geral de Proteção de Dados (LGPD)
Orientador(a): Liz Beatriz Sass

Eu, Johann Bielemann Cunha, acima qualificado(a); venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 24 de setembro de 2021.

_____

Johann Bielemann Cunha

AGRADECIMENTOS

Chega ao fim um ciclo, muito maior que os cinco anos (e meio) dispostos para a conclusão da faculdade, mas sim um ciclo que se iniciou na pré-escola e encerra-se (até o momento) com a graduação em Direito. Com toda certeza somos eternos aprendizes, sendo a caminhada do aprendizado muito mais prazerosa na companhia destes gigantes profissionais e seres humanos, os professores, aos quais exponho o meu mais sincero agradecimento.

Agradeço especialmente aos meus pais, por todo incentivo, amor, compreensão e por demonstrar o papel fundamental da educação. Vocês são sem dúvidas meus maiores exemplos!

Agradeço aos meus amigos, os quais não listarei nominalmente pois com certeza esquecerei de algum. Vocês foram fundamentais para tornar leve esta longa caminhada. À minha namorada, Isabela Mello, pelo amor, apoio e compreensão, principalmente durante este último ano dedicado à vida profissional e acadêmica.

Agradeço ao advogado Paulo Vidigal, que prontamente disponibilizou sua recente obra, esta que viria a ser a principal condutora deste estudo. E, por fim, à minha orientadora, Dra. Liz Beatriz Sass, por confiar no meu projeto mesmo que o prazo fosse curto, compartilhando comigo toda sua experiência acadêmica.

RESUMO

O presente trabalho tem como objetivo analisar a base legal do legítimo interesse no âmbito da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18), demonstrando as hipóteses de sua utilização e as balizas para sua adequada aplicação. O avanço tecnológico pode ser considerado um dos combustíveis da discussão da privacidade, uma vez que cria novos meios de interagir com a sociedade. Para a edição da LGPD não foi diferente, diversos escândalos de vazamento de dados culminaram em um movimento mundial pela proteção de dados. Contudo, este movimento preocupando-se em não frear a inovação e o desenvolvimento econômico, estabeleceu diversas hipóteses em que o tratamento de dados pessoais é autorizado: as bases legais. Dentre estas situações, chama especial atenção a permissão do tratamento de dados pessoais baseado no legítimo interesse do agente de tratamento, de forma que a vontade da figura central da lei, o titular dos dados, é deixada em segundo plano. Partindo de uma análise bibliográfica acerca do tema, fazendo um paralelo com as normas de outros sistemas jurídicos, assim como com as leis brasileiras anteriores à LGPD, e utilizando do método dedutivo, esta pesquisa foi dividida em três capítulos. O primeiro capítulo traz uma breve conceituação de privacidade, além de demonstrar o contexto histórico em que a lei foi editada, por fim, aprofundando-se nos princípios que devem ser observados durante as atividades de tratamento de dados pessoais. No segundo capítulo, discorre-se sobre a importância da correta escolha da base legal, bem como, sobre as particularidades de cada uma. Por fim, dedica-se no último capítulo ao exame da base legal do legítimo interesse e os critérios que devem ser observados para sua adequada utilização. Assim, conclui-se que o legítimo interesse goza da mesma força que as demais bases legais e que, embora flexível, não se caracteriza como uma permissão absoluta para o tratamento de dados pessoais.

Palavras-Chaves: Legítimo Interesse. Dados Pessoais. Legítima Expectativa. LGPD.

ABSTRACT

The current study aims to analyze the legal basis of the legitimate interest in the scope of the Brazilian General Law for the Protection of Personal Data (Law n. 13.709/18), demonstrating the hypotheses of its use and the guidelines for its proper application. Technological advancement can be considered one of the fuels in the discussion of privacy, as it creates new ways to interact with society. For the LGPD edition it was no different, several data leakage scandals culminated in a worldwide movement for data protection. However, this movement, concerned not to stop innovation and economic development, established several hypotheses in which the processing of personal data is authorized: the legal bases. Among these situations, special attention is drawn to the permission to process personal data based on the legitimate interest of the processing agent, so that the will of the central figure of the law, the personal data subject, is left in the background.

Based on a bibliographical analysis on the subject, making a parallel with the norms of other legal systems, as well as with Brazilian laws prior to the LGPD, and using the deductive method, this research was divided into three chapters. The first chapter provides a brief conceptualization of privacy, in addition to demonstrating the historical context in which the law was enacted and going deeper into the principles that must be observed during personal data processing activities. The second chapter discusses the importance of choosing the correct legal basis, as well as the particularities of each one. Finally, the last chapter is dedicated to examining the legal basis of legitimate interest and the criteria that must be observed for its proper use. Thus, it is concluded that the legitimate interest enjoys the same force as other legal bases and that, although flexible, it is not characterized as an absolute permission for the processing of personal data.

Keywords: Legitimate Interest. Personal data. Legitimate Expectation. LGPD.

SUMÁRIO

1. INTRODUÇÃO

A abrupta mudança tecnológica vivida nos últimos 100 (cem) anos não foi acompanhada pela devida conscientização da população de qual é o motor desta nova revolução. Se antes tínhamos o carvão e o petróleo como combustíveis da sociedade moderna, hoje, graças ao enorme poder matemático e computacional disposto, os dados tornaram-se uma valiosa *commodity* para empresas e governos.

Em um mundo globalizado com mais de 7 (sete) bilhões de pessoas, uma categoria de dados ganha especial relevância, os dados pessoais. Contudo, essa relevância surge muito antes do avanço tecnológico da sociedade, estando presente desde os primórdios da humanidade, pelo seu grande valor para a atividade mercantil.

Neste viés, o dado pessoal não deve ser visto como somente aquele que prontamente permite a identificação de determinada pessoa, como um nome ou o CPF, mas todo aquele que diz respeito à esta pessoa, por exemplo, matrícula da faculdade, horário de saída do serviço, hábitos alimentares, dentre infinitas informações relacionadas a uma pessoa que, combinadas, permitem sua identificação.

O conceito de tratamento de dados pessoais igualmente não pode ser limitado a popular ideia de que somente existe tratamento de dados pessoais quando utilizado grande poder intelectual ou computacional. Nesta esteira, o simples armazenamento ou transferência de um dado pessoal já é considerado tratamento, sendo certo que diariamente todos nós tratamos dados pessoais.

Desta forma, buscando ganhar vantagens competitivas, as empresas passaram a cada vez mais interessar-se em acumular estes dados pessoais, criando verdadeiros *data-banks* de informações de seus clientes, fornecedores e colaboradores, muitas vezes sem qualquer utilidade imediata aparente. Não demorou muito tempo para essa acumulação desenfreada de dados pessoais conflitar com os direitos dos titulares de dados pessoais.

Vazamentos de vídeos, espionagem de chefes de Estado[1], venda de dados pessoais por parte do Facebook para gigantes da tecnologia[2], a sensação de monitoramento constante a todo e qualquer site acessado na internet, estas e muitas

---

[1] ENTENDA o caso de Edward Snowden, que revelou espionagem dos EUA. G1, 2013. Disponível em: < http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou- espionagem-dos-eua.html>. Acesso em: 22 de ago. de 2021

[2] ENTENDA o caso de Edward Snowden, que revelou espionagem dos EUA. G1, 2013. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2018/12/19/facebook-compartilhou-mais-dados-com-gigantes-tecnologicos-do-que-o-revelado-diz-jornal.ghtml>. Acesso em: 22 de ago. de 2021

outras situações chamaram atenção do mundo para a falta de segurança com que os dados pessoais são tratados. A fragilidade e descuido com estes dados começou a causar um movimento mundial, inclusive legislativo, a fim de garantir que esses, importantes para empresas, mas que não a elas pertence, sejam tratados com a maior segurança possível, com o intuito de tornar o titular dos dados o agente com mais força nessa relação.

No período entre os primeiros seminários acerca do tema, das primeiras consultas públicas aos projetos de lei, até a aprovação de uma lei que viesse a dar guarida a estes dados, houveram diversos escândalos como os anteriormente citados, gerando uma maior atenção e técnica legislativa para abordar o tema, desaguando na publicação em 14 de agosto de 2018 da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/18, pondo fim, ou, pelo menos sendo considerada fruto de mais de uma década de debates acerca da necessidade de proteção de dados no Brasil.

Todavia, a proibição absoluta ao tratamento de dados pessoais nunca foi uma possibilidade, uma vez que tal prática está enraizada em diversos serviços e produtos utilizados pela população, sendo certo que referida proibição ocasionaria um retrocesso à sociedade. Assim, na mesma linha de outras leis de *Compliance*, a LGPD traduz-se muito mais em uma lei principiológica do que em uma lei proibitiva e sancionatória.

É possível notar que dentre as diversas possibilidades em que a lei autoriza o tratamento de dados pessoais, muitas delas são para situações específicas onde o consentimento do titular dos dados se mostra claramente desnecessário, pois incompatível com o objetivo almejado, como é o caso do tratamento de dados para execução de contratos. Fácil de se imaginar, não poderia um colaborador recusar que seus dados sejam tratados e exigir receber seu salário, pois para alcançar-se o pagamento é necessário o tratamento dos dados pessoais.

Não obstante, além do consentimento e das situações específicas para a qual a lei previu uma autorização para o tratamento dos dados pessoais, visando: a) não esgotar as hipóteses de tratamento um rol taxativo e; b) prever um dinamismo para o tratamento de dados pessoais, evitando que para todo e qualquer tratamento fosse necessário obter o consentimento do titular, o legislador, igualmente ao que fez o legislador da *General Data Protection Regulation (GDPR)* – Regulamento de Proteção de Dados Europeu, introduziu a possibilidade de utilização do legítimo interesse como justificativa para o tratamento de dados pessoais, permitindo que em determinadas

hipóteses seja possível o tratamento sem que haja a necessidade da coleta do consentimento, visando muitas vezes, fins comerciais do controlador.

Diante do exposto, busca o presente trabalho, a partir do método dedutivo e de pesquisa bibliográfica e documental, demonstrar que o legítimo interesse goza da mesma força que as demais bases legais e que, embora flexível, não se caracteriza como uma permissão absoluta para o tratamento de dados pessoais.

Assim, no primeiro capítulo, serão analisados conceitos fundamentais da Lei Geral de Proteção de Dados (LGPD), que servirão de base para a compreensão de toda a exposição deste trabalho. Em seguida, no segundo capítulo, adentrar-se-á nas hipóteses autorizadoras de tratamento de dados pessoais, explicitando em quais cenários cada uma delas melhor se enquadra, bem como, suas forças e fraquezas.

Por fim, no terceiro capítulo, será estudada a base legal do legítimo interesse, demonstrando os critérios que devem ser obedecidos para sua utilização, demonstrando que esta base legal goza da mesma força que as demais bases legais, vez que não se traduz em permissão absoluta para o tratamento de dados pessoais.

2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Embora não seja essencial que o operador do direito seja um especialista em tecnologia da informação para entender a LGPD, a compreensão de determinados conceitos o ajudará a expandir seu entendimento sobre a mesma.

Conforme preconiza Maldonado (2019, p.12), embora os esforços das mais diversas regulamentações sobre proteção de dados pessoais, vive-se em um mundo de *big data*, onde estas informações são processadas por todos, pelas empresas ou pelas próprias pessoas, e a todo momento, em um volume jamais antes visto.

Os estudos sobre privacidade embora tenham ganhado contorno mais acentuado na era da informação, estão presentes desde a antiguidade, como é possível ser visto na distinção Aristotélica entre vida pública e vida privada, ou *polis* e *oikos*, respectivamente. Contudo, como vivemos em uma sociedade dinâmica e, para garantir a efetividade da proteção à privacidade, qualquer definição, natureza e mecanismos desta proteção devem ser constantemente atualizadas (MALDONADO, 2019, p.12).

Desde do famoso ensaio *The Right of Privacy* de Samuel Warren e Louis Brandeis (1890, p. 193), passou-se a compreender a privacidade com um direito individual. No artigo, os autores surpreendiam-se com as novas tecnologias, questionando até que ponto, as recém chegadas máquinas fotográficas, por exemplo, poderiam adentrar em domínios até então invioláveis da vida privada. Nos dias atuais não é diferente, o avanço da tecnologia é um dos principais responsáveis pelo avanço nas discussões acerca da privacidade.

O simples conhecimento de que a todo momento suas informações são processadas por numerosos agentes e que, deste processamento, decisões, muitas vezes automatizadas, são tomadas, sem qualquer participação ativa do dono titular de dados pessoais, colocou este em uma posição de passividade. Como leciona Bioni (2019, p. 39), há uma “economia de vigilância”, onde o titular transforma-se em um mero expectador do fluxo de seus dados, estes que são a base de sustentação deste novo mercado.

Nesta sociedade informacional, a geração de riqueza está na observância dos comportamentos de cada indivíduo que, somadas, são capazes de construir padrões e tornar a mensagem publicitária cada vez mais eficiente (BIONI, 2019, p.64). Além da publicidade, aparentemente sutil, tornar-se gradativamente mais agressiva, uma vez que considera todos seus padrões de consumo, o contínuo processamento de

dados pessoais pode ser utilizado para os mais diversos fins, desde segurança pública até práticas discriminatórias, colocando os cidadãos em um panóptico, como mera matéria-prima para essa rede de atores.

Bioni (2019, p.64) leciona que é essencial a conciliação entre os interesses econômicos destes atores e o empoderamento do titular dos dados pessoais no controle sobre estes. Este é o cerne para o sucesso de qualquer legislação que venha a regular o tema, a inobservância de qualquer um destes dois aspectos acarretará o fracasso da lei.

2.1 CONTEXTO HISTÓRICO

Com o pós-guerra, o mundo concentrou seus esforços em estabelecer direitos mínimos a todas os cidadãos, sendo fruto destes esforços a elaboração da Declaração Universal de Direitos Humanos [3], documento do qual já era possível extrair preocupações com a privacidade:

> Artigo 12 - Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Esta diligência com a privacidade foi constantemente aperfeiçoada, inclusive tendo sido transposta no art. 5º, inciso X, da nossa Constituição Federal de 1988, que estabelece que “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”. Contudo, conforme acentua Viviane Maldonado (2019, p. 13), para entender a evolução legislativa que deu a autonomia aos dados pessoais, torna-se importante a compreensão de dois instrumentos da legislação europeia: a) a Carta dos Direitos Fundamentais da União Europeia de 2000, artigo 8º; e b) o Tratado de Funcionamento da União Europeia (TFUE), artigo 16, ambas que preconizam que “Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito”.

Esta emancipação do direito à proteção dos dados pessoais do direito à privacidade (Maldonado, 2019, p. 13), somada a um contexto de grande fluxo de dados e a tentativa de, naquele momento, diversos estados membros da União Europeia de instituírem diretivas próprias relacionadas à proteção destes dados,

[3] Disponível em: < https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acessado em: 22 de ago. de 2021.

escancarou a necessidade da edição de uma lei única que viesse a dar segurança jurídica aos seus jurisdicionados, o que trouxe a devida relevância para a discussão da temática.

Foi nesta conjuntura que em 2012 iniciou-se o trâmite da proposta de criação de um Regulamento Geral Europeu que viesse a ser aplicável a todos os estados-membros. Aprovada em abril de 2016 e com início de sua eficácia em 2018, a *GDPR (General Data Protection Regulation)* uniu todas as normas relativas ao tema de forma coesa, aplicando inclusive extraterritorialidade nos casos em que o agente de tratamento ofertar produtos ou serviços à União Europeia ou tratar os dados pessoais de seus residentes (Maldonado, 2019, p. 14). Além disso, houve a imposição de restrições às contratações das empresas europeias que, a partir daquele momento, somente poderiam contratar empresas de países estrangeiros se no país do contratado houvesse grau de proteção similar ou superior ao estabelecido pela lei, o que naquela época excluía o Brasil (Oliveira, 2020, p. 30). Desta forma, houve um forte efeito em cascata na cadeia de fornecimento das empresas europeias, tendo o Brasil ainda em 2018 promulgado a Lei Geral de Proteção de Dados – LGPD (Lei 13.709/18).

Contudo, quando a LGPD foi aprovada, o Brasil não estava completamente desamparado no assunto de proteção aos dados pessoais, uma vez que já existia no país lei para dar guarida a parte destas relações, trata-se do Marco Civil da Internet – MCI (Lei 12.965/2014) e seu Decreto Regulador (Decreto 8.771/2016).

2.1.1. Marco Civil da Internet – MCI

Conforme preconiza Palhares, Prado e Vidigal (2021, p. 33), para o correto entendimento do Marco Civil da Internet, necessário se faz relembrar qual era o contexto na época de sua aprovação. Em 2013, o mundo chocava-se com o vazamento de grande parte de documentos de espionagens realizadas pelo Estados Unidos, divulgados pelo então ex-agente da CIA, Edward Snowden. Nos documentos restou claro que o Brasil vinha sendo um dos focos desta vigília, inclusive tendo o e-mail da então Presidente Dilma Rouseff sido alvo desta espionagem.

Ademais, ressalta Bioni (2019, p. 186) que à época tentava-se criar uma lei com traços do direito criminal para regular o uso da internet, através de uma técnica legislativa que seria prescritiva e restritiva das liberdades individuais, o que viria a travar qualquer inovação advinda da internet e teria consequências sociais e

econômicas devastadoras.

Com esta recente demonstração de vulnerabilidade aos quais os dados pessoais, inclusive da presidente do país, estavam expostos e, com a ausência de uma lei específica que viesse a dar o adequado resguardo à essas situações, o Brasil aprovou em 23 de junho de 2014 o Marco Civil da Internet, a fim de regular o uso da internet.

Já é possível encontrar no MCI conceitos importantes que foram posteriormente aproveitados na elaboração da LGPD, destaca-se "especialmente os de "dados pessoais" e de "tratamento"[4], a privacidade como um princípio[5], direitos dos usuários, padrões de segurança para guarda, armazenamento e tratamento de dados pessoais[6]" (OLIVEIRA, 2020, p.35), bem como, diversos princípios que balizam atualmente o tratamento de dados pessoais.

Dos princípios estabelecidos pelo Artigo 3º do MCI, dois deles demonstram especial relevância para a posterior compreensão da LGPD e do papel do legítimo interesse, são eles: a) inciso III – proteção dos dados pessoais, na forma da lei; e b) inciso VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios da lei.

Conforme dispõe Palhares, Prado e Vidigal (2021, p.36), a menção explícita ao termo "na forma da lei", é fruto de discussões que já rondavam o tema naquela época, com o entendimento de que se fazia necessária a edição de uma outra lei que

---

[4] Art. 14. Para os fins do disposto neste Decreto, considera-se:
I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
II - tratamento de dados pessoais - 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.

[5] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;

[6] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e
IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

disciplinasse especificamente a proteção de dados pessoais. Assim, devemos lembrar que o MCI não visava especializar-se no regulamento do tratamento de dados pessoais, mas apenas ganhou comandos para assegurar alguns direitos inerentes à navegação na internet (Palhares, Prado e Vidigal, 2021, p.36), estes que tangem à proteção dos dados pessoais.

Verifica-se no próximo princípio que uma lei que seja desconexa da realidade econômica tende ao fracasso. A garantir a liberdade dos modelos de negócio promovidos na internet o legislador prestigiou a inovação e a livre-iniciativa, evitando que a internet brasileira tivesse características típicas de regimes totalitários (Palhares, 2021, p. 39).

Outros contornos relativos ao direito de proteção de dados podem ser encontrados no Marco Civil Internet, especialmente em seu art. 7º. Em seu inciso VII[7] c/c IX[8], já via-se a necessidade do consentimento expresso e informado, destacado das demais cláusulas contratuais, para hipóteses em que a lei não autorizava o tratamento. Logo depois, no inciso VIII[9] do referido artigo, contornos do princípio da finalidade, da legalidade e dos direitos dos titulares mostravam-se presentes, bem como, a necessidade de registro destas operações. Por fim, o direito do titular de ter seus dados excluídos tão logo a relação entre as partes tenha terminado ou a seu simples requerimento, nos ditames do inciso X[10].

Malgrado o microssistema de proteção de dados pessoais existente na lei, fato é que o MCI e seu Decreto regulamentador são insuficientes para regular o tratamento de dados pessoais como um todo, uma vez que todos seus aspectos são aplicáveis somente nas relações que ocorrem no ambiente virtual, mais especificamente durante o uso da Internet (Oliveira, 2020, p. 37). Inclusive, é o que se extrai da redação do seu Art. 1º:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso

---

[7] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
VII - 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;

[8] IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

[9] VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

[10] X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

> da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Embora não possa ser descartada a contribuição do MCI para a proteção de dados pessoais, as disposições do artigo 7º "mais atrapalham do que ajudam na almejada segurança jurídica, tanto aos usuários quanto aos provedores, pois ao passo em que a LGPD traz, por exemplo, 10 hipóteses para o tratamento de dados, o MCI limita tal possibilidade ao consentimento" (Palhares, Prado e Vidigal, 2021, p. 49).

Neste viés, conforme expõe Palhares, Prado e Vidigal (2021, p. 49), é possível compreender que o MCI como norma regulamentadora do tratamento de dados pessoais foi completamente suplantada com a entrada em vigor da LGPD, respeitando-se o princípio da especialidade[11] – *lex specialis derogat legi generali* (a lei especial derroga a lei geral).

Buscando enterrar qualquer discussão sobre a aplicabilidade ou não da LGPD ao tratamento de dados no ambiente virtual, o próprio artigo 1º da lei estabelece de forma expressa que:

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

Importante salientar que com o advento da LGPD não ocorre a revogação completa do MCI, sendo esta última a lei que permanece a regular o uso da internet, entretanto, no que se refere à regulamentação do tratamento de dados pessoais, inclusive na internet, a lei aplicável será a LGPD. Enquanto não ocorrem todas as correções e revogações por meio legislativo, cabe à doutrina e à jurisprudência gradualmente apaziguar o conflito entre ambas (Palhares, Prado e Vidigal, 2021, p. 50). Ainda, sobre a superação da microssistema de proteção de dados da MCI frente a LGPD, ressalta Marcel Leonardi (2020, p.241):

> A LGPD é apenas uma lei "geral" em oposição a uma lei "setorial": é lei específica sobre proteção de dados pessoais e aplicável de modo uniforme, horizontal e geral a toda e qualquer atividade de tratamento, realizada por toda e qualquer entidade pública ou privada, por qualquer meio, ressalvadas as exceções previstas em lei.
> Por fim, quando comparada ao MCI, é evidente que a LGPD representa lei especial, regulando de modo pormenorizado todas as atividades de

[11] LINDB - Art. 2º Não se destinando à vigência temporária, a lei terá vigor até que outra a modifique ou revogue.
§ 1º A lei posterior revoga a anterior quando expressamente o declare, quando seja com ela incompatível ou quando regule inteiramente a matéria de que tratava a lei anterior.

> tratamento de dados pessoais, enquanto o MCI trata de diversos outros temas distintos, como neutralidade de rede, salvaguardas de responsabilidade civil e regras específicas para a remoção de conteúdo de plataformas online. Nesse contexto pelo critério da especialidade, a LGPD igualmente prevaleceria sobre os dispositivos sobre proteção de dados pessoais do MCI.

Contudo, Palhares, Prado e Vidigal (2021, p. 53), apesar de concordar com a hierarquia da LGPD frente a MCI quando o assunto é proteção de dados pessoais, assevera que os dispositivos que não demonstrem incompatibilidade com a nova lei permanecem vigentes, devendo ser interpretados como complementares à própria LGPD.

2.1.2 Vacatio Legis da LGPD

Como ressaltado, o cenário externo com a edição da *GDPR* em 2016 e o escândalo da *Cambridge Analytica*[12] foram catalisadores para a promulgação em agosto de 2018 da Lei Geral de Proteção de Dados (Lei 13.709), com previsão para vigorar a partir do mesmo mês de 2020. A partir deste momento iniciava-se uma corrida para que todas as empresas se adequassem à nova legislação.

Prontamente, com a edição da lei eleva-se a reputação brasileira a fim de permitir o fluxo de dados pessoais entre Brasil e União Europeia. Ainda, a similaridade entre a lei brasileira acabou sendo extremamente vantajosa para o estudo sistemático e comparado da proteção de dados pessoais, de modo que, como se está alguns meses atrás, constantemente nos aproveita-se suas diretivas, jurisprudências e doutrina (Maldonado, 2019, p.15).

Contudo, por fatores externos, como a pandemia de Covid-19 (SaRS-CoV-2), e fatores internos, como a pressão de alguns setores para obter mais tempo à adequação, a vigência da lei foi adiada por outras duas oportunidades, tendo a lei entrado em vigor somente 18 de setembro 2020 e suas punições apenas a partir de 1º de agosto de 2021. Assim, hoje pode-se afirmar que a Lei Geral de Proteção de Dados Pessoais – LGPD está plenamente em vigor, embora lacunas permaneçam sem respostas pela Autoridade Nacional de Proteção de Dados – ANPD, como será

[12] Durante investigações sobre interferência estrangeira nas eleições dos EUA, ocorridas em novembro de 2016, o FBI e os órgãos de inteligência do país descobriram que a empresa britânica Cambridge Analytica — contratada pelo então candidato Donald Trump — teria coletado dados pessoais de mais de 87 milhões de norte-americanos. Os especialistas constataram que as informações, com preferências e perfis de opinião de usuários norte-americanos do Facebook, foram decisivas para a vitória de Trump. Disponível em: <https://cfa.org.br/de-onde-veio-a-lgpd/>. Acessado em: 24/08/2021.

exposto adiante.

2.2 DADOS PESSOAIS E SEUS TITULARES

Conforme assevera Oliveira (2020, p. 43), um leigo ao ouvir pela primeira vez sobre a LGPD, tende a pensar que ela protege igualmente os dados empresarias, tanto os segredos de negócio como os dados identificadores, como CNPJ, endereço, data de constituição, dentre outros. Contudo, em uma leitura mais atenta, verifica-se que a legislação visa tutelar tão somente os dados pessoais, o que não necessariamente exclui dados que possam igualmente dizer respeito à pessoas jurídicas.

Oliveira (2020, p. 43) traz importante reflexão sobre a qual bem jurídico cada lei visa proteger. Deste modo, o Direito Penal, por exemplo, em alguns artigos visa tutelar a vida (homicídio, Art. 121, CP) e, em outros, a própria propriedade (furto, Art. 151, CP), entre outras disposições. A Constituição em seus arts. 5º, XIII, 6º e 7º, estabelece o trabalho como um fundamento da República Federativa do Brasil, tendo normas que proíbem trabalho infantil, forçado e com carga superior ao permitido em lei. Visa-se, com tais dispositivos, a proteção da saúde do trabalhador, ainda, assegurando o seu convívio social. Da mesma forma, ressalta-se a lição de Ricardo Oliveira e Márcio Cots:

> O principal bem jurídico resguardado pela LGPD é a privacidade. Ao contrário das pessoas jurídicas, as pessoas naturais (de carne e osso) se formam durante a vida e necessitam de ambiente propício para seu desenvolvimento, mas tal ambiente não é gerado por si mesmas. (...) A importância da privacidade para o desenvolvimento humano é atestada pelas grandes religiões da humanidade, pois, via de regra, há sempre momentos em que o retiro, seja para o deserto, seja para dentro de si mesmo, é essencial para a construção do ser humano e sua visão de si mesmo. (OLIVEIRA e COTS, 2020, p. 44)

A proteção da privacidade visa proteger o desenvolvimento do ser humano, conforme dispõe Norbert Elias em “A Sociedade dos indivíduos” (1994), um recém-nascido não é mais que o esboço preliminar de uma pessoa, que desenvolverá sua personalidade das relações entre ela e sociedade. Deste modo, a LGPD dedicou-se a preservar os dados pessoais das pessoas naturais, visando à tutela da privacidade destas, uma vez que pessoas jurídicas não gozam deste tipo de proteção.

Conforme dispõe Palhares, Prado e Vidigal (2021, p. 117), há exceções no direito empresarial brasileiro que muitas vezes levam a confundir uma pessoa jurídica com uma pessoa física (natural), criando uma zona cinzenta para definir-se a

abrangência do conceito de “titular de dados”. Tem-se como exemplos o Empresário Individual e do Microempreendedor Individual (MEI), que muitas vezes realizam o registro no Cadastro Nacional de Pessoas Jurídicas meramente para fins tributários. Para estes casos, como o ordenamento jurídico dá a estes tipos empresariais classificação jurídica de pessoas naturais, deste modo, “exige-se o mesmo grau de cautela e conformidade com a LGPD que aqueles dados das pessoas naturais convencionais” (Palhares, Prado e Vidigal, 2021, p. 118).

Para iniciar propriamente a discussão do alcance da LGPD, importante destacar o conceito de dado pessoal e de titular de dados elencados na lei:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Prontamente observa-se que a LGPD, igualmente ao que faz a GDPR, não trouxe um rol taxativo do que se constitui um dado pessoal, de modo que a avaliação se determinada informação consiste ou não como um dado pessoal deve ser sempre realizada de maneira contextual. (Maldonado, 2019, p.15). A título exemplificativo, o número de matrícula de um funcionário sem nenhuma outra informação pode nada representar, contudo, este número dentro do contexto da organização facilmente leva a identificação de uma pessoa, devendo este dado ser tratado nos termos da lei. Sobre a análise contextual, ressalta Felipe Palhares, Luis Prado e Paulo Vidigal:

> “No campo prático, o conceito de dado pessoal vai além daqueles dados comumente utilizados em cadastros (como nome, endereço, profissão, documentos de identidade) e, na maioria das vezes, inclui qualquer tipo de informação que possa ser útil à individualização de uma pessoa natural (física), como conjunto de hábitos, comportamentos, preferências, registros eletrônicos (inclusive dados de acesso e uso de internet). Trata-se portanto, de um conceito aberto, sendo praticamente impossível cravar se determinado dado é ou não pessoal sem a análise do contexto em que se insere.” (PALHARES, PRADO e VIDIGAL, 2021, p. 117)

Quanto a propriedade destes dados, é certo dizer que ela nunca é transmitida do titular ao agente de tratamento, o que o agente possui é tão somente um direito de uso sobre os mesmos (Oliveira, 2020, p. 45). Assim, mesmo que uma empresa utilize de esforços para a coleta e manutenção de dados pessoais de acordo com a legislação, estes nunca a ela pertencerão, sendo a titularidade mantida na pessoa natural (Palhares, Prado e Vidigal, 2021, p. 117).

2.2.1 Dados pessoais sensíveis

Categoria especial criada pelo legislador e que merece atenção neste momento inicial são os dados pessoais sensíveis. Expressa no Art. 5º, II, em um rol aparentemente taxativo, a definição de dado pessoal sensível foi criada para dar guarida àquelas informações mais íntimas de cada titular ou que em determinadas ocasiões, infelizmente, ainda são utilizadas para discriminá-lo.

> 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;

Os dados acima elencados devem, salvo exceções, ser interpretados como sensíveis, o que limitará suas hipóteses de tratamento. Contudo, embora tenha o legislador buscado a criação de um rol taxativo, a análise contextual far-se-á necessária para identificar se determinado dado pessoal é sensível ou não. O jurista Luis Fernando Prado Chaves[13] já ressaltou, por exemplo, que, para PEPs (Pessoas Politicamente Expostas) é inadequado considerar o dado de filiação à organização de caráter política como um dado pessoal sensível:

> "o controle e a ampla difusão dos atos dos políticos pela sociedade contra resguardo na Constituição Federal, é a base dos princípios republicanos e democráticos que estão em nossa Constituição Federal (vide artigo 5º, XXXIII da Constituição Federal) e não poderia ser restringido pela LGPD. Assim, considerando o objetivo da LGPD ao prever um regime especial para os dados sensíveis, parece certo que, no caso dos políticos, a filiação partidária não carrega o mesmo potencial crítico/discriminatório como ocorre no caso de cidadão comum."

É neste viés que se reafirma a necessidade de considerar o contexto da atividade de tratamento no momento de categorizar um dado pessoal, evitando-se uma interpretação binária da Lei, pois tal ato poderá vir a desvirtuar os objetivos legais (Palhares, Prado e Vidigal, 2021, p. 120).

De maneira breve, é importante salientar que para efetivação de uma melhor proteção aos dados sensíveis, as bases legais para o tratamento – que serão vistas mais a frente – desta categoria de dado são ainda mais restritas (Art. 11º), inclusive não havendo previsão que autorize o tratamento com base no legítimo interesse, motivo pelo qual não aprofundar-se-á na distinção entre o dado pessoal "comum" e o dado pessoal sensível.

---

[13] Disponível em <https://lgpdrive.com.br/cap-i-arts-1%C2%BA-6%C2%BA#h.nz-lj92xk0zak>. Acessado em 30 de mar. de 2021.

2.2.2 Tratamento de dados pessoais

Para a correta compreensão da lei é necessário emancipar-se da ideia de que o tratamento de dados pessoais pressupõe complexo poder computacional ou matemático. Em verdade, o conceito de tratamento é bastante amplo, inclusive sendo considerado como exemplificativo o rol trazido pela definição da lei (Art. 5º, X):

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

Em qualquer das hipóteses acima mencionadas ocorre o tratamento de dados pessoais, mas não somente, conforme assevera Palhares, Prado e Vidigal (2021, p. 121) a mera visualização ou acesso aos dados pessoais já pode ser considerada tratamento, seja em meio digital ou físico, devendo serem observadas as disposições da lei.

Para facilitar a compreensão do limite da definição de tratamento, dá-se o exemplo de um empregador e seu funcionário. Neste exemplo, durante o prazo de vigência do contrato, o empregador terá de realizar o tratamento de dados pessoais do colaborador por diversos motivos, como: pagamento de salário, controle do ponto, adimplemento de verbas previdenciárias, concessão do benefício do plano de saúde, dentre outros. Os dados em si podem ser os mais variados, seguindo-se o exemplo acima, o empregador terá de guardar o número da conta do empregado, o horário de chegada do mesmo, o número da CTPS e o nome dos filhos e cônjuge dependentes. Ainda, caso o funcionário venha a ser desligado, o empregador deverá guardar, no mínimo, durante o prazo prescricional trabalhistas, alguns destes dados, por exemplo, controle do ponto e dados cadastrais básicos. Toda atividade em que dados pessoais sejam manuseados, são consideradas tratamento, inclusive sua retenção, devendo o agente de tratamento para todo tratamento observar a lei.

2.3 PRINCÍPIOS FUNDAMENTAIS

A técnica legislativa utilizada na LGPD foi adequada no que concerne à sobrevida da lei ao tempo, uma vez que invés de optar por uma lei restritiva e punitiva, o legislador buscou a elaboração de uma lei principiológica, característica inerente às leis de *Compliance*. Considerando-se que a LGPD é uma lei que impactará tanto o setor público quanto o privado, empresas dos mais diversos ramos nas quais só

recentemente as reflexões sobre proteção de dados pessoais ganharam especial atenção, a adoção de princípios pelo legislador foi a melhor opção para garantir a eficácia da lei (Palhares, Prado e Vidigal, 2021, p. 129). Segundo a doutrina, princípios podem ser entendidos como normas balizadoras para qualquer operação jurídica:

> "princípios, no plural, significam as normas elementares ou os requisitos primordiais instituídos como base, como alicerce de alguma coisa [...] revelam o conjunto de regras ou preceitos, que se fixam para servir de norma a toda espécie e ação jurídica, traçando, assim, a conduta a ser tida em qualquer operação jurídica [...] exprimem sentido mais relevante que o da própria norma ou regra jurídica [...] mostram-se a própria razão fundamental de ser das coisas jurídicas, convertendo-se em perfeitos axiomas [...] significam os pontos básicos, que servem de ponto de partida ou de elementos vitais do próprio Direito." (SILVA, De Plácido. 2001, p. 639)

Com a escolha por uma lei principiológica, a LGPD é capaz de se torna referência à produção de leis posteriores que venham a tutelar hipóteses de tratamento específicas, ou ainda, auxiliar na interpretação de outras normas que tenham como tema o tratamento de dados pessoais (Oliveira, 2020, p. 42).

Embora os princípios sejam norteadores da aplicação da lei, sendo muito mais flexíveis, a jurisprudência europeia demonstra que parcela relevante das penalidades são tomadas com base na violação destes (Palhares, Prado e Vidigal, 2021, p. 131). Conforme levantamento de sanções aplicadas pelas autoridades europeias[14], já são 160 multas aplicadas pela simples não observância de princípios, que somadas, perfazem o valor de mais de 780 milhões de euros.

Dissertar-se-á sobre todos os princípios estabelecidos na LGPD, contudo, será de extrema importância a compreensão de determinados princípios para a discussão do legítimo interesse, são eles: a) Princípio da boa-fé; b) princípio da finalidade; c) princípio da adequação; d) princípio da necessidade e; e) princípio da transparência.

2.3.1 Princípio da boa-fé

O primeiro princípio consagrado no *caput* do Art. 6º da LGPD é amplamente encontrado em diversas outras legislações, caracterizando-se igualmente como princípio basilar do direito brasileiro, o princípio da boa-fé. Embora sempre exista notória subjetividade na aplicação deste conceito, importante ressaltar que a lei alberga a noção de boa-fé objetiva, que utiliza o homem-médio como parâmetro para

[14] GDPR Enforcement tracker: insights. Disponível em <https://www.enforcementtracker.com/?insights>. Acessado em 29 de ago. de 2021.

estabelecer a conduta esperada.

Conforme discorre Palhares, Prado e Vidigal (2021, p. 131), em grandes organizações a boa-fé transcende a noção do cumprimento do comando jurídico, já que, por vezes, o mercado é muito mais exigente que a própria legislação e se baliza por noções éticas, uma vez que o simplesmente cumprimento da lei não se mostra suficiente.

É por este motivo que o Comitê Consultivo da Convenção 108 recomenda que controladores de dados pessoais estabeleçam governança independente para identificarem valores éticos que necessitam de proteção no contexto das atividades de tratamento de dados que conduzem[15].

Em sede de proteção de dados, pode-se entender o princípio da boa-fé como um princípio maior, do qual se desdobram alguns dos demais princípios, cita-se os princípios: da finalidade, da transparência e da necessidade. Conforme se verá adiante, todos estes princípios são desdobramentos de um compromisso maior de coerência, da boa-fé do agente de tratamento.

2.3.2 Princípio da finalidade

Um dos princípios mais importantes consignados na LGPD é o princípio da finalidade (Art. 6º, I), que estabelece que:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

Deste princípio é possível desprender-se outros, como a legalidade e a transparência, contudo, o alicerce do princípio da finalidade reside no fato de os controladores de dados não poderem tratar os dados pessoais para meramente satisfazer seus desejos, devendo o tratamento possuir uma finalidade específica, esta que deverá ser documentada no relatório de operações de tratamento (Palhares, Prado e Vidigal, 2021, p. 132).

Conforme assevera Doneda (2015, p.378), o princípio da finalidade traz a

---

[15] CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, p. 5. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a>. Acessado em 29 de ago. de 2021.

característica inerente da disciplina de proteção de dados, uma vez que o tratamento dos dados pessoais sempre estará de estar vinculado à finalidade que originou sua coleta. A finalidade para o tratamento de um dado pessoal deve ser a mesma que originou sua coleta, de modo que, havendo alteração desta, haverá de ser analisado a compatibilidade que eventualmente poderá suscitar providências por parte do controlador, como, por exemplo, informar o titular dos dados da nova finalidade para a qual seu dado será utilizado, ocasionalmente trocar a base legal que fundamenta o tratamento, dentre outras (Palhares, Prado e Vidigal, 2021, p.132).

Neste sentido, a Opinião do *Working Party* 29 sobre o princípio da finalidade e a necessidade de compatibilidade entre os tratamentos:

> Mais do que impor um requerimento de compatibilidade, o legislador escolheu uma dupla negação: assim, proibiu a incompatibilidade. Se a norma autorizasse o tratamento posterior desde que não incompatível (e mediante o preenchimento dos demais requisitos de licitude), daria a impressão de que o legislador teria pretendido conferir flexibilidade com relação ao uso posterior. Tal uso pode ser bastante próximo do propósito inicial ou razoavelmente diferente. O fato de que o tratamento posterior mira um propósito diferente não necessariamente significa que é automaticamente incompatível com o original: é preciso verificar essa questão à luz do caso concreto[16].

Ainda, sobre a compatibilidade de finalidades determinados pontos devem ser observados para a evitar o descumprimento da lei:

> Na análise da compatibilidade de propósito secundário em relação ao original deve-se medir (i) a relação entre os propósitos original e secundário (quanto maior a distância entre eles, menor a chance de compatibilidade); (ii) o contexto da coleta de dados e a razoável expectativa dos titulares envolvidos com relação a eventual uso secundário dos dados (quanto mais inesperado ou surpreendente o uso secundário, mais improvável a compatibilidade); (iii) a natureza dos dados tratados e o impacto do uso secundário para os titulares (quanto mais sensíveis os dados envolvidos, menor a margem de compatibilidade); e (iv) as medidas tomadas pelo agente de tratamento para garantir o tratamento justo e mitigar eventuais riscos. (PALHARES, PRADO e VIDIGAL, 2021, p. 134)

Por fim, no momento da definição da finalidade do tratamento é importante ressaltar que esta não pode ser genérica, devendo trazer determinado grau de especificidade. Como exemplifica Palhares, Prado e Vidigal (2021, p.133), a

---

[16] ARTICLE 29 WORKING PARTY: *Opinion 03/2013 on purpose limitation, p. 21*. Tradução livre. Redação original: *Rather than imposing a requirement of compatibility, the legislator chose a double negation: it prohibited incompatibility. By providing hat any further processing is authorized as long as it is not incompatible (and if the requirements of lawfulness are simultaneously also fulfilled), it would appear that the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different. The fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis.* Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em 29 de ago. 2021.

famigerada “melhoria na experiência do usuário” aqui não cabe, sendo necessário mais detalhes para, neste exemplo, trazer maiores detalhes como a coleta de determinado dado pessoal melhorará a experiência do titular.

2.3.3 Princípio da adequação

Apesar de muito similar ao princípio da finalidade, o princípio da adequação estabelece que deve haver “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (Art. 6º, II).

Todavia, conforme destaca Palhares, Prado e Vidigal (2021, p. 134), há uma nuance que não pode ser desconsiderada, quando ambos princípios falam sobre a compatibilidade, tutelam momentos diferentes, enquanto o princípio da finalidade se preocupa com a compatibilidade do tratamento posterior, o da adequação tutela a compatibilidade no tratamento original.

Além disso, o princípio da adequação requer a análise se o tratamento dos dados que estão sendo solicitados aos titulares é adequado à finalidade perseguida. A título exemplificativo, imagina-se que para um determinado sorteio, seja necessário o titular dos dados informar seu celular. Neste caso, vemos que é completamente adequado que o controlador trate este dado, pois essencial para o atingimento da finalidade informada ao titular. Contudo, o tratamento de dados não relevantes para o atingimento da finalidade informada, como, por exemplo, do número de integrantes da família do titular, tornará o tratamento incompatível. Neste ponto, o princípio da adequação aproxima-se muito do próximo princípio a ser estudado, o princípio da necessidade.

2.3.4 Princípio da necessidade

Seguindo a corrente de princípios, o princípio da necessidade surge para acabar com uma prática que vinha sendo cada vez mais utilizada pelos agentes de tratamento, a coleta indiscriminada de dados pessoais para justificar uma futura e incerta utilidade. Neste viés, estabelece o Art. 6º, III:

> 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;

Muito ligado ao princípio da finalidade, uma vez que antes da definição da

quantidade mínima de dados para alcançar determinado objetivo é necessário delimitar qual é este fim (Palhares, Prado e Vidigal, 2021, p. 135), o princípio da necessidade faz com que as organizações reflitam sobre a necessidade de coleta, processamento e retenção de determinados dados. Com o advento da LGPD, a manutenção de dados pessoais desnecessários às finalidades imediatas acaba por simplesmente gerar riscos empresariais que devem ser prontamente mitigados.

Para Palhares, Prado e Vidigal (2021, p.135), perguntas devem ser feitas para analisar a necessidade ou não do tratamento de determinado dado pessoal, são elas: a) De quais dados pessoais necessitamos para atingir os propósitos do tratamento? b) Seria possível realizar a atividade com menos dados?; c) Seria possível aplicar técnicas como pseudonimização ou anonimização aos dados definidos como necessários (por exemplo, utilizar iniciais em vez de nome completo ou informações generalizadas em vez de individualizadas)?; e d) Ao término do tratamento, atingida a finalidade, há alguma razão para a não exclusão de dados? Por quê? Se sim, por quanto tempo devemos retê-los até que possamos finalmente excluí-los?

Conforme destaca Vainzof (2019, p. 114), políticas empresarias que visem reter o máximo de dados possíveis estão fadadas a serem consideradas ilícitas, uma vez que o princípio da necessidade impõe uma cultura de minimização de dados. Assim, havendo outros meios de se atingir a finalidade pretendida, o tratamento de dados pessoais será questionável.

Assim como os demais princípios, a análise do princípio da necessidade deve ser feita constantemente, uma vez que após atingida a finalidade perde-se muitas vezes a necessidade de retenção de determinado dado. Uma empresa madura é capaz de enxergar o princípio da necessidade como uma vantagem para seu negócio, uma vez que seus atributos resultaram em redução de custos e um maior nível de assertividade[17].

2.3.5 Princípio da transparência

A saída do titular da posição passiva em que era mantido antes da LGPD inicia a partir do momento em que o controlador é obrigado a dispor, de maneira clara, informações ao titular acerca do tratamento que pretende realizar. Para Palhares,

[17] FORBES. *Why Data Minimization is an Important Concept in the Age of Big Data.* 16.03.2016. Disponível em: <https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=7cfa26b11da4>. Acessado em: 30 de ago. de 2021.

Prado e Vidigal (2021, p. 137) é somente com a garantia da transparência que o titular passa a exercer controle sobre o fluxo de suas informações.

Contudo, não basta a elaboração de uma política de privacidade extensa escondida atrás de diversos *links* de acesso, é necessário que os controladores inovem e pensem em maneiras de realmente garantir que o titular dos dados tenha ciência e aceite o tratamento posto, caso contrário, o princípio da transparência não estará sendo cumprido.

O Art. 9º da lei é categórico em estabelecer de maneira clara características sobre o tratamento que devem ser disponibilizados ao titular:

> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

As técnicas para garantir a transparência do tratamento são as mais diversas, desde *checkboxes* desmarcados, adoção de técnicas de *legal design* e *visual law*, até chegar a vídeos exclusivos para explicar a dinâmica do tratamento. Deste modo, conforme destaca Vainzof (2019, p. 116), a informação disponibilizada ao titular de dados sobre o tratamento deverá ser prestada de forma sucinta e eficaz, evitando-se a “fadiga informacional”.

Em uma acepção ética em que “tudo que não puder contar como fez, não faça”, discorre-se sobre o princípio da transparência:

> “a transparência, do ponto de vista do agente de tratamento de dados, funciona como espécie de filtro quanto à razoabilidade e à licitude da atividade. Ora, se o ente que realiza o tratamento de dados não sente o conforto necessário para expor suas atividades de tratamento de forma transparente e aberta publicamente, ressalvadas as hipóteses de sigilo admitidas pelo Direito deveria servir para trazer dúvida sobre a própria licitude da atividade”. (PALHARES, PRADO e VIDIGAL, 2021, p. 138).

Assim, o princípio da transparência deixa de ser útil apenas para o cumprimento dos requisitos da LGPD e para a efetivação dos direitos dos titulares, mas torna-se útil para o controlador refletir sobre a própria licitude de suas atividades (Palhares, Prado e Vidigal, 2021, p. 139). Em caso da ocorrência de incidentes de segurança ou violação aos direitos dos titulares, todos os esforços envidados pela controladora

serão levados em consideração tanto pelo judiciário, quanto pela agência reguladora.

2.3.6 Demais princípios

A escolha por deixar os outros princípios agrupados não advém da menor importância que possuem, mas de simples liberalidade, por entender que será proveitoso para a compreensão do legítimo interesse, objeto deste trabalho, o aprofundamento em cada um deles. Contudo, a observância dos princípios acima mencionados não basta para que o agente de tratamento esteja completamente diligente com a lei, conforme observaremos.

Existem ainda princípios ligados ao resultado do tratamento, como o princípio da qualidade, que determina que os dados pessoais tratados devem ser exatos, claros, relevantes e atualizados, e o princípio da não-discriminação, que estabelece que é vedado o tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos. A inobservância destes princípios no momento do tratamento será catastrófica para o agente de tratamento, uma vez que poderá implicar em reais prejuízos para o titular de dados pessoais (Palhares, Prado e Vidigal, 2021, p. 137).

Por outra linha, princípios ligados a segurança e diligência na retenção dos dados devem ser igualmente observados, como é o caso do princípio da segurança (Art. 6, VII) e princípio da prevenção (Art. 6º, VIII). O primeiro diz respeito a responsabilidade que o agente de tratamento deve ter ao projetar suas defesas, considerando a complexidade do seu negócio, volume de dados pessoais tratados e tecnologias envolvidas, para garantir que o ambiente de tratamento seja seguro. Por sua vez, o princípio da prevenção nos leva a uma mitigação prévia do risco de violação destes dados pessoais, como o estabelecimento de boas-práticas, elaboração de relatórios de impacto e comunicação proativa à agência reguladora em caso de incidentes (Palhares, Prado e Vidigal, 2021, p. 139).

O princípio do livre acesso, muito conectado ao princípio da transparência, é essencial para colocar o titular dos dados pessoais no centro da relação, garantindo que estes possam consultar facilmente as informações sobre o tratamento, bem como, a integralidade de seus dados pessoais que estão sob posse do agente de tratamento.

Por fim, em conjunto os princípios da responsabilização e prestação de contas, demonstrando a necessidade de o agente de tratamento demonstrar sua conformidade, não somente no papel, mas o cumprimento e monitoramento efetivo das regras de tratamento. Para Palhares, Prado e Vidigal (2021, p. 142), é preferível que em estágios iniciais de maturidade é preferível o estabelecimento de poucas

regras que sejam efetivamente cumpridas, do que a elaboração de documentos e estrutura complexa que não saem do papel, nos moldes do Art. 50, §2[18].

Nunca é muito lembrar que a retenção de dados pessoais também é considerada um tratamento e, caso não seja capaz de adimplir com um dos princípios acima mencionados, o tratamento deve cessar ou ações devem ser imediatamente tomadas. Tal qual como mencionado quando se explicava o princípio da necessidade, o agente de tratamento deve a todo momento reavaliar se o tratamento para o qual se propõe está adequadamente atendendo a todos princípios estabelecidos na lei.

2.4 OS AGENTES DE TRATAMENTO E A AGÊNCIA REGULADORA (ANPD)

Conceituada a figura central da LGPD, o titular de dados, necessário aprofundar-se no destinatário final da lei – os agentes de tratamento – que deverão alinhar seus comportamentos às disposições da mesma. De forma breve, a Lei Geral de Proteção de Dados distribuiu em duas figuras as atribuições destes agentes: O controlador (Art. 5º, VI) e o operador (Art. 5º, VII).

O controlador é o agente de tratamento que determina as diretrizes do tratamento, Palhares, Prado e Vidigal (2021, p. 121) traz como exemplo: a escolha de quais dados coletar, por qual motivo coletar, como utilizar, por quanto tempo armazenar, para quais finalidades, etc. Porquanto, o operador será aquele que, obedecendo às ordens do controlador, realizará o tratamento. Dispensadas discussões aprofundadas sobre um caso concreto, um exemplo prático da atividade

[18] § 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.

de operador é quando uma empresa de pesquisa é contratada por uma outra empresa (controladora) para coletar dados pessoais específicos. É certo dizer que nesta situação hipotética, o operador não possui qualquer gerência sob os dados, somente disponibilizando seus meios e *expertise* para o atingimento dos fins perseguidos pela controladora.

Antes de aprofundar-se nas responsabilidades de cada agente, necessário expor que em suma, o empregado de determinada empresa não é considerado operador de dados pessoais, porquanto é mero recurso da organização, sendo que está sim deve ser considerada um operador ou controlador (Palhares, Prado e Vidigal, 2021, p. 121). Sobre o tema:

> "Em primeiro lugar, diga-se que, apesar da confusão que vem sendo feita sobre essa questão no Brasil, em regra, não faz sentido, dentro de uma mesma organização, falar em divisão de enquadramento entre controladores e operadores de acordo com as funções exercidas. Ora, a organização não existiria não fossem as pessoas físicas que para e por ela desempenham suas funções (que, por sua vez, não são controladores nem operadores), nem as pessoas estariam exercendo suas atividades não fosse o objeto social perseguido pela empresa". (PALHARES, PRADO e VIDIGAL, 2021, p. 121)

Embora os empregados não sejam caracterizados como agentes de tratamento, há exceção quanto um colaborador exerce atividade de tratamento que destoa dos objetivos da empresa, para fins próprios, situação em que poderá vir a ser considerado como agente controlador autônomo (Palhares, Prado e Vidigal, 2021, p. 122), o que não elidirá a responsabilidade da empresa pela utilização do dado pessoal para fins distintos do que informado ao titular de dados.

Similar ao que ocorre no princípio da responsabilidade e prestação de contas, não adianta as atribuições de cada partes estarem definidas em contrato, com distribuição de reponsabilidades, meios de tratamento e requisitos de segurança, se a realidade verificada for diversa do que previamente acordada.

Por fim, é necessário enxergar o dinamismo das relações hodiernas, nem sempre o fornecedor ou o prestador de serviço será o operador, nem o agente que coleta o dado pessoal e o transmite será considerado controlador, vide exemplo de empresa de pesquisa dado anteriormente. Embora ainda não disciplinada expressamente na LGPD, tanto a doutrina quanto a lei europeia aceitam pacificamente o conceito de cocontrole, onde ambas as partes agem como controladoras dos dados pessoais (Palhares, Prado e Vidigal, 2021, p. 122).

2.4.1 Agência Nacional de Proteção de Dados (ANPD)

A ANPD, por sua vez, é a agência reguladora pública criada para zelar, implementar e fiscalizar o cumprimento da LGPD no país (Palhares, Prado e Vidigal, 2021, p. 125). Conforme rememora Gutierrez (2019, p. 316), a ANPD será uma agência reguladora capaz de permear todos os setores econômicos da sociedade, inclusive a própria Administração, motivo pelo qual é imprescindível que a mesma seja dotada de autonomia para exercer seu poder fiscalizatório.

O Art. 55-J da LGPD busca concentrar estas competências, entre as quais merecem destaque: a) fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento da legislação (inciso IV); b) promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais (inciso VI); c) editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais (inciso XIII); e d) deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da Lei, as suas competências e os casos omissos (inciso XX).

Como será exposto no último capítulo deste trabalho, existe relevante discussão sobre a obrigatoriedade ou não da elaboração prévia do Relatório de Impacto à Proteção de Dados (RIPD), bem como, seu conteúdo. Deste modo, deverá a ANPD debruçar-se sobre este tema e emitir seu parecer.

Embora a ANPD possua o poder de fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento com a legislação, Gutierrez (2019, p. 322) faz importante ponderação:

> A fiscalização e possibilidade de aplicação de sanções é parte essencial da institucionalização da proteção dos dados pessoais materializada pela criação da ANPD. Mas é necessário que se construa um arcabouço de estímulo às boas práticas por parte das organizações de modo a reduzir ao máximo a necessidade de se recorrer ao expediente da punição. Nesse campo, a publicação de diversos guias, orientações e estudos por parte da ANPD pode trazer uma baliza importante para que controladores e operadores possam adequar suas práticas e processos internos da maneira mais eficiente possível de modo a evitar que sejam alvo de processos administrativos e, eventualmente, de sanções.

As competências da ANPD são as mais diversas e estão espalhadas por toda lei, em síntese, é importante lembrar que a lei foi editada com diversas lacunas que remetem à uma futura regulamentação desta agência. Assim, a ANPD possui um papel fundamental para que a lei tenha plena eficácia, prestando esclarecimentos sobre os pontos controvertidos da lei, a exemplo do que faz o Conselho Europeu de Proteção de Dados (EDPB) relativamente à GDPR.

3. AS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Aos leigos, a chegada de uma lei que visava regular o tratamento de dados pessoais pode dar a impressão de que o legislador buscava proibir o tratamento de dados pessoais no Brasil, no entanto, qualquer visão neste sentido está completamente equivocada. A intenção da LGPD nunca foi proibir ou dificultar o tratamento de dados pessoais, mas apenas definir as “regras do jogo” (Palhares, Prado e Vidigal, 2021, p. 144).

Importante salientar que com o advento da nova disciplina, o agente de tratamento está obrigado a encontrar ao menos uma base legal que autorize sua atividade de tratamento. Destaca-se que a “base legal nada mais é do que um motivo justo e lícito, aos olhos da legislação para que os dados pessoais possam ser tratados” (PALHARES, PRADO e VIDIGAL, 2021, p. 144), deste modo, caso não seja possível enquadrar o tratamento em nenhuma das bases jurídicas, o mesmo deve ser imediatamente interrompido.

Quando o MCI (Marco Civil da Internet) e seu decreto regulador eram consideradas as principais normas relativas à proteção de dados pessoais, persistia uma visão “consentimentocentrista”, onde o consentimento era considerado o único meio pelo qual o controlador de dados pessoais estava autorizado a realizar um tratamento. Com o advento da LGPD, houve significativa evolução quanto a este pensamento, pois – seguindo a lógica do velho continente – ampliou-se o rol de hipóteses autorizadoras ao tratamento de dados pessoais (Palhares, Prado e Vidigal, 2021, p. 144), tornando a lei aderente à realidade social.

A emancipação do consentimento não ocorreu da noite para o dia, mas foi fruto de constante evolução da técnica legislativa. Sobre este desprendimento, assevera Bioni:

> É interessante notar que, na primeira versão do anteprojeto de lei colocada sob consulta pública em 2010, o consentimento era, em termos topográficos, a única base legal para o tratamento de dados pessoais. Isso se repetiu na segunda consulta pública em 2015, quando o que hoje são as demais bases legais da LGPD eram hipóteses nas quais o consentimento poderia ser dispensado.
> Após tais consultas públicas, o texto enviado ao Congresso Nacional, que depois veio a ser aprovado e sancionado, acabou por posicionar o consentimento como sendo uma das hipóteses legais e não na cabeça do dispositivo. Isso significa que, em termos de técnica legislativa, **o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais por estarem todos elas horizontalmente elencadas em incisos do art. 7º da LGPD**. (BIONI, Bruno. 2019, p.188) (Grifo nosso)

Porém, antes de adentrar na explanação sobre cada uma das bases legais, é importante salientar que a lei estabeleceu abordagem diferenciada para os dados pessoais “comuns” e os dados pessoais “sensíveis”. Enquanto que para o tratamento de dados pessoais “comuns” existem 10 (dez) bases legais autorizadoras, para o tratamento de dados pessoais sensíveis há apenas 8 (oito) hipóteses (Oliveira, 2020, p. 48), dentre as quais o consentimento ganha especial relevância. Tal relevância pode ser observada pela técnica legislativa utilizada, uma vez que estabelece que o “tratamento de dados pessoais sensíveis somente poderá ocorrer” em dois casos: a) com o consentimento específico e destacado do titular de dados (Art. 11, I) e; b) sem o consentimento do titular quando o tratamento for indispensável para uma das sete hipóteses elencadas pela lei (Art. 11, II). Ainda, sempre importante ressaltar que dentre as hipóteses elencadas para a supressão do consentimento no tratamento de dados pessoais sensíveis não figura o legítimo interesse.

Não obstante, conforme assevera Palhares, Prado e Vidigal (2021, p. 144), o correto enquadramento do tratamento em uma base legal ainda é um desafio, uma vez que a doutrina nacional é escassa e a agência reguladora não emitiu diretrizes neste sentido. Para contornar este problema, observa-se que os profissionais de proteção de dados buscam constantemente recorrer à doutrina europeia, com a observância das diretrizes produzidas pelas autoridades reguladoras atuantes nestes países para, desta forma, garantir a conformidade de suas empresas/clientes.

3.1 A importância da correta definição da base legal

Garantir que o tratamento de dados pessoais esteja amparado em um base legal é mais do que uma boa prática do controlador de dados, mas uma obrigação, pois são elas que legitimarão a atividade como um todo. Assim, deve o controlador ter clareza quanto a sua escolha, sendo considerado um bom primeiro-passo a observância dos princípios do Art. 6º da LGPD (Palhares, Prado e Vidigal, 2021, p. 145).

A preocupação do controlador de dados em utilizar uma base legal para legitimar o seu tratamento já é um bom indício de boa-fé (Art. 6º, *caput*), desde que em conjunto com a base legal haja o cumprimento dos demais princípios. Igualmente neste viés, verifica-se na primeira parte da definição do princípio da finalidade (Art. 6º, I) a necessidade de o tratamento ser para propósitos legítimos, de modo que, um dos

pressupostos de legitimidade é a existência de uma base legal (Palhares, Prado e Vidigal, 2021, p. 145).

Em outros casos, a correta escolha da base legal pode iluminar o caminho para o cumprimento de um princípio, como ocorre com o princípio da necessidade (Art. 6º, III). É que ao observar o comando legal, o controlador é capaz de observar o mínimo de dados pessoais que será necessário coletar. Por exemplo, um empregador ao fornecer os dados de seu colaborador para o INSS, quando requisitado por este, sabe exatamente o limite dos dados que deverão ser transferidos, de modo que não deverá passar nenhum dado que não seja solicitado pelo órgão, sob pena de estar extrapolando a base legal do cumprimento de obrigação legal (Art. 7º, II) e realizando um tratamento desnecessário, em violação ao princípio da necessidade.

A depender da base legal utilizada, faz-se necessário maior ou menor atenção ao princípio da transparência (Art. 6º, VI), conforme exemplifica Palhares, Prado e Vidigal, “impõe-se especial atenção à transparência quando o tratamento for realizado com base no legítimo interesse (art. 10, §2)” (2021, p. 146). Sempre importante rememorar que a transparência exigida na LGPD não obriga o controlador a transmitir a informação técnica-jurídica da base legal que fundamenta o tratamento, mas sim do modo que este é realizado.

O tratamento deverá ser documentado no Relatório de Operações de Tratamento ou ROPA (*Relatory of Processing Activities),* que nada mais é que um documento que traz todas as informações necessárias sobre os dados pessoais que transitam em cada fluxo. Neste relatório sim, faz-se importante a presença da base legal escolhida, pois referido documento pode ser solicitado pela autoridade nacional para comprovar a conformidade do agente. É neste diapasão que mais um princípio surge conectado à obrigação de escolha da base legal, o princípio da prestação de contas (Art. 6º, X).

Entender qual a base legal que legitima o tratamento é importante para diversas outras aplicações, uma delas, é a retenção após alcançada a finalidade que inicialmente autorizou o tratamento, como é o caso da retenção de dados para cumprimento de obrigação legal ou regulatória (Art. 16, I). Utilizando do mesmo exemplo supracitado, é necessário que o empregador guarde determinadas informações do colaborador, como ficha ponto, dados cadastrais, dentre outros, mesmo após o desligamento deste, Caso o controlador de dados pessoais no momento do tratamento original entendesse que a base legal que fundamenta o

tratamento não encontra respaldo nas hipóteses de conservação do Art. 16[19], provavelmente iria se expor a riscos com a eliminação equivocada dos dados (Palhares, Prado e Vidigal, 2021, p. 146).

Esta definição sempre será realizada pelo controlador de dados e não pelo operador, pois é o primeiro quem define as diretrizes estratégicas do tratamento, bem como, na maioria das vezes, possui contato com o titular de dados pessoais. Por este motivo, é comum e indicado que os operadores no momento do contrato com o controlador, estabeleçam cláusula no sentido de que a responsabilidade pelo atendimento aos direitos dos titulares, bem como, da garantia de que o tratamento está devidamente fundamentado em uma base legal é do controlador (Palhares, Prado e Vidigal, 2021, p. 147).

Felipe Palhares, Luis Prado e Paulo Vidigal (2021, p. 147) compartilham a experiência de que em algumas empresas a definição da base legal é descentralizada da área de privacidade, alocando esta responsabilidade na área dona do fluxo. Contudo, esta estratégia gera diversas dificuldades, dentre elas, a necessidade de um aprofundado treinamento da lei para as mais diversas áreas, o que com certeza não é produtivo. Para os autores, esta estratégia pode ser utilizada, no entanto, faz-se necessária uma dupla verificação do time de privacidade para garantir que a base legal indicada pela área está adequada com a realidade do processo.

3.2 As bases legais: suas forças e fraquezas

Antes de indicar a base legal que fundamentará o tratamento, algumas considerações necessitam ser feitas quanto a natureza deste, pois, conforme certas particularidades, a LGPD indicará se uma base pode ou não ser utilizada.

O primeiro aspecto a ser observado é: Quem é o agente de tratamento? Isso decorre do fato de algumas bases legais terem sido pensadas exclusivamente para alguns agentes, como é o caso da base legal da tutela da saúde (Art. 7º, VIII), que expressamente indica que o procedimento deve ser realizado por profissional da saúde, serviços de saúde ou autoridade sanitária. Há ainda, outros exemplos, como a

[19] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

base legal que autoriza o tratamento para realização de estudos por órgãos de pesquisa (Art. 7º, IV), sendo estes órgãos considerados aqueles da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos que tenha em sua missão institucional, objetivo social ou estatutário, a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Por fim, ainda na observância do agente de tratamento, há a execução de políticas públicas como hipótese autorizadora (Art. 7º, III) que, conforme expressamente previsto pela lei, só pode ser utilizada pela administração pública.

Como previamente mencionado, a natureza dos dados também influencia na escolha da base legal. A não diferenciação entre “dado pessoal” e “dado pessoal sensível” pode fazer com que o agente de tratamento realize um processamento de dados ilícitos, uma vez que nem todas as bases legais disponíveis para “dados pessoais” podem ser utilizadas para justificar o tratamento de “dados pessoas sensíveis” (Palhares, Prado e Vidigal, 2021, p. 148).

Há também a necessidade de observar-se características do titular dos dados, dentre os mais importantes a idade. Pela redação do Art. 14, §1, o tratamento de dados pessoais de crianças e adolescentes só pode ser realizado com consentimento específico e destacado de um dos pais ou do responsável legal, salvo exceções previstas no §3[20] do mesmo artigo.

O art. 5º, X traz diversas hipóteses não exaustivas do que pode ser considerado um tratamento, dentre estas hipóteses está a transferência, que merece especial atenção. Para além dos cumprimentos das bases legais ordinárias do Art. 7º ou 11º, o Art. 33 e ss. da lei estabelece condições que devem ser observadas no caso de transferências internacionais (Palhares, Prado e Vidigal, 2021, p. 148).

Assim, antes de adentrar em cada uma das hipóteses autorizadoras do tratamento de dados pessoais, apresenta-se importante lição de Felipe Palhares, Luís Prado e Paulo Vidigal que funciona como um guia para definição da base legal:

> (i) **é ideal a eleição de uma única base legal para cada tratamento** (ainda que, no caso concreto, possa haver certa sobreposição e/ou convivência de bases);
> (ii) **nenhuma base legal é mais importante ou melhor do que outra**. Trata-se de cardápio de hipóteses alternativas, cuja aplicação dependerá do propósito perseguido pela atividade de tratamento, bem como das circunstâncias destacadas anteriormente;

[20] § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

> (iii) a rigor, as bases legais requerem que o tratamento seja necessário para o atingimento de determinado propósito (seja, por exemplo, o cumprimento de uma norma ou a execução de um contrato). Assim, se for possível atingir o propósito sem realizar o tratamento, é provável que não se encontre uma base legal para este;
> (iv) é recomendável que as bases legais sejam determinadas, de maneira documentada, anteriormente ao tratamento, haja vista que cada uma delas produz uma gama de efeitos próprios, os quais podem demandar ajustes nas atividades e providências a serem previamente endereçadas pelos agentes de tratamento;
> (v) não há obrigação legal expressa para que se informe a base legal ao titular de dados pessoais, já que a base legal não é um dos critérios consagrados no artigo 9º da LGPD;
> (vi) após a definição, a rigor, não se deve trocar de base legal, sob pena de ser verificar que o enquadramento inicial foi feito erroneamente, deflagrando irregularidade da operação até então; e
> (vii) em caso de modificação do propósito para tratamento de dados pessoais, será preciso avaliar se é possível sustentar o tratamento na base originalmente definida, o que passa pela análise de compatibilidade do novo propósito com o anterior. (PALHARES, PRADO e VIDIGAL, 2021, p. 149) (Grifo Nosso)

Realizadas as considerações iniciais sobre as bases legais e a importância do correto enquadramento do tratamento, cabe agora compreender quando cada uma das hipóteses previstas no Art. 7º deve ser utilizada.

3.2.1 Consentimento

Embora não seja o objeto deste trabalho, importante debruçar-se de maneira mais atenta sobre a base legal do consentimento, uma vez que há notória preferência dos agentes de tratamento pela escolha desta em detrimentos das demais bases, o que não deveria ocorrer. Há de ser considerar a recente história legislativa, não podendo culpar os agentes de tratamento pela preferência da base legal do consentimento, já que há pouco tempo, no MCI por exemplo, verificava-se o consentimento como salvaguarda central para permitir o tratamento de dados pessoais.

Neste sentido, importante destacar que “o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais por estarem todos elas horizontalmente elencadas em incisos do art. 7º da LGPD” (BIONI, Bruno. 2019, p. 188).

Conforme referido anteriormente, a escolha da base legal deve ser única, no entanto, observa-se um movimento de empresas utilizando o consentimento como uma espécie de reforço, para garantir a licitude do tratamento. Neste sentido, a

autoridade nacional de proteção de dados grega já aplicou penalidade à empresa de auditoria que utilizava o consentimento para tratamento de dados pessoais de colaboradores[21]. Em sua defesa, a empresa alegou que o consentimento era apenas utilizado como um "reforço", argumento que foi desmontado pela autoridade grega (Palhares, Prado e Vidigal, 2021, p. 154). Esta ideia está completamente equivocada, como se verá a seguir, o consentimento pode ser um fardo na vida do agente de tratamento.

Assim, sob perigo de retroceder à época de insegurança jurídica, faz-se importante que os agentes de tratamento reconheçam a horizontalidade de todas bases legais, reconhecimento este que só será alcançado com forte atuação da doutrina, da autoridade reguladora, como foi o caso da punição atribuída pela autoridade grega, e, principalmente, da jurisprudência.

Adentrando na definição do consentimento para a LGPD, a lei estabelece que consentimento como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Art. 5º, XII). Verifica-se forte ligação da necessidade de o consentimento ser "informado" com o princípio da transparência, ora, conforme lição de Bruno Bioni (2019, p.191): "(...) apenas com uma informação adequada o cidadão estará capacitado para controlar seus dados".

Quanto a necessidade de o consentimento ser "livre", verifica-se uma das maiores dificuldades para operacionalização desta base legal, motivo pela qual ela não deve ser a primeira opção do agente de tratamento. A própria LGPD traz em seu art. 8, §3 a vedação do tratamento de dados pessoais com vício do consentimento, vício este que alude as hipóteses previstas no Código Civil, como erro, dolo, coação, estado de perigo e lesão.

Não obstante, constata-se também situações em que o titular de dados está em um estado de vulnerabilidade em relação ao agente de tratamento que solicita seu consentimento, por exemplo, relações empregatícias e contratos de adesão (Palhares, Prado e Vidigal. 2021, p. 157). Sobre esta hipótese, importante manifestação do *Working Party 29*:

> Dada a dependência presente na relação entre empregador e empregado, é improvável que o titular de dados seja capaz de negar ao seu empregador o consentimento para o tratamento de seus dados pessoais sem que

[21] GDPR Enforcement Tracker, ETid 65. Disponível em: <https://www.enforcementtracker.com/ETid-65>. Acesso em 03.09.2021

> experencie medo ou risco real de prejuízo. É improvável que um empregado possa responder livremente a uma solicitação de consentimento de seu empregador, por exemplo, no que diz respeito ao monitoramento por câmeras do ambiente de trabalho ou ao preenchimento de formulário de avaliações, sem sentir pressão para consentir. Portanto, o WP29 entende problemático o tratamento de dados pessoais de atuais ou futuros empregados por parte do empregador com base no consentimento, já que este provavelmente não será livre. Para a maioria das atividades de tratamento de dados relacionados ao trabalho, a base legal aplicável não deve ser o consentimento dada a natureza do relacionamento entre empregador e empregado[22].

Seguindo, “inequívoco” se refere ao fato de que o silêncio não importante consentimento do titular, contudo, também não há formalidades para obtenção do consentimento desde que esse constitua-se como uma ação afirmativa do titular (Palhares, Prado e Vidigal. 2021, p. 158).

Assim verifica-se que a escolha pelo consentimento significa dar máximo poder ao titular de dados pessoais durante toda a relação, como exemplifica Palhares, Prado e Vidigal: “o agente de tratamento tem de estar preparado para: 1) o titular negar autorização e a atividade não ocorrer; 2) o titular revogar o consentimento, no meio do caminho, interrompendo a atividade.” (2021, p. 163). Não estando o agente de tratamento confortável com a escolha do tratamento estar em sua totalidade na mão do titular de dados pessoais, deve se voltar a atenção para as demais bases legais.

3.2.2 Cumprimento de obrigação legal ou regulatória

A redação desta base legal acaba por ser autoexplicativa e determina que sempre que houver a necessidade de tratamento de dados pessoais para o cumprimento de uma obrigação legal, o agente de tratamento estará autorizado a fazê-lo. Contudo, recorda-se que independentemente da base legal escolhida, todos os princípios têm de ser observados. Nesta base legal em específico, chama-se atenção ao princípio da necessidade, que estabelece que o agente de tratamento

---

[22] ARTICLE 29 WORKING PARTY. *Guidelines on consente under Regulation 2016/679,* p. 7. Tradução livre. Redação original: *Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as cameraobservation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. 18 Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee*
Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>. Acessado em: 04 de set de 2021.

deve limitar o tratamento ao mínimo necessário para o atendimento da finalidade que, neste caso, guarda relação com o comando legal (Palhares, Prado e Vidigal, 2021, p. 168).

Para evitar confusões, importante destacar que obrigações contratualmente assumidas não se enquadram no presente inciso, não podendo relações privadas serem invocadas para justificar o tratamento de dados pessoais (Lima, 2019, p. 138). É importante que os operadores de dados pessoais tomem a devida diligência antes de assumir obrigações de tratamento, exigindo que o controlador dos dados pessoais garanta que cumpriu com todos os princípios no momento da coleta dos dados pessoais, garantindo inclusive a existência de uma base legal que fundamente o tratamento.

Conforme assevera Palhares, Prado e Vidigal (2021, p.169) considera-se uma boa-prática inclusive que o agente de tratamento verifique a regularidade formal do comando a ser atendido, analisando-o sob a ótica do titular dos dados, que nesta relação estará em uma posição de extrema vulnerabilidade, uma vez que, possivelmente, sequer possui conhecimento do comando legal. Neste sentido, a juíza da 5ª Vara da Fazenda Pública do município de São Paulo deferiu tutela de urgência suspendendo a exigência de que a *Uber* compartilhasse informações sensíveis de seus motoristas com a prefeitura, pois, entendeu que o município não tomará todas as providências necessárias para garantir o sigilo e segurança destes dados pessoais[23]. Da decisão, extrai-se o seguinte trecho:

> "Com efeito, resta evidente o risco de que os dados sigilosos dos parceiros da autora sejam indevidamente acessados por terceiros, causando prejuízos não só a eles próprios, como também à requerente, na medida em que eles se constituem em fonte de planejamento estratégico e comercial da empresa(...). Desta feita, defiro a tutela de urgência para o fim de suspender, por ora, a obrigação da autora de remeter as informações relativas aos seus parceiros ao Município de São Paulo(...)[24]"

Igualmente temos sempre que lembrar que a sociedade é mutável, motivo pelo qual é possível que algum tratamento realizado com fundamento em outra base legal possa vir a ser enquadrado futuramente como cumprimento de obrigação legal. Por exemplo, no momento em que vivemos algumas cidades estão exigindo o chamado "passaporte vacina" para acesso a eventos. Ora, é certo que se antes não havia

---

[23] MIGALHAS. *Uber não é obrigado a compartilhar dados pessoais com prefeitura de SP.* 25.01.2018. Disponível em: <https://www.migalhas.com.br/quentes/273078/uber-nao-e-obrigado-a-compartilhar-dados-pessoais-com-prefeitura-de-sp> Acessado em: 07 de set. de 2021.

[24] Processo nº 1002511-62.2018.8.26.0053

fundamento para exigir a comprovação da vacinação de determinado titular, agora se tem a obrigação de coletar tal dado, da mesma forma caso tais decretos venham a ser revogados, o tratamento deva ser interrompido imediatamente.

3.2.3 Execução de contrato

A base legal da execução de contrato torna-se essencial para evitar engessar a livre iniciativa e o dinamismo das relações contratuais, contudo, sua indevida utilização não será suportada pela agência reguladora. Extrai-se da lei:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> 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**; (Grifo nosso)

Do primeiro grifo, extrai-se que o tratamento de dados pessoais necessita guardar estrita relação com a execução do contrato, não sendo suficiente a mera inclusão de cláusula que informe tratamento de dados que não guarde relação com o fim almejado pelo contrato. Desta disposição, extrai-se que "o texto contratual não pode artificialmente expandir a categoria de dados ou tipos de tratamento necessários para que o contrato seja adequadamente executado" (PALHARES, PRADO e VIDIGAL, 2021, p. 174).

Sobre o elemento da necessidade de o tratamento guardar relação com o contrato, extrai-se opinião do *Working Party 29*:

> (...) deve ser interpretado de maneira estrita e não abrande situações em que o tratamento não é, de fato, necessário para a execução de contrato, mas exigência unilateral imposta ao titular dos dados pessoais por parte do controlador. Além disso, o simples fato de o tratamento ter sido contemplado no contrato não significa, automaticamente, que se faz necessário à sua execução (...) Ainda que as atividades de tratamento de dados sejam especificamente mencionadas no texto do contrato, isso, por si só, não as torna 'necessárias' para a execução do contrato[25].

Por conseguinte, importante destacar que para a correta utilização da base

---

[25] ARTICLE 29 WORKING PARTY. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects,* p. 9. Tradução Livre. Redação Original: (…) *must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance. […] Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract*. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en>. Acessado em 07 de set. 2021.

legal da execução de contrato, faz-se necessário que o titular dos dados pessoais seja parte na relação firmada, não bastando ser mero representante legal, sendo certo que, segundo Palhares, Prado e Vidigal (2021, p. 172), neste caso, estar-se-á diante de hipótese de tratamento de dados baseado no legítimo interesse.

3.2.4 Exercício regular de direitos

Para além das bases legais acima aventadas, o legislador previu como hipótese autorizadora de tratamento o "exercício regular de direitos em processo judicial, administrativo ou arbitral", em uma noção antagônica ao abuso de direito. Esta base legal, prevista no Art. 7º, inciso VI, torna-se importantíssima no que tange a guarda de dados, conforme assevera Felipe Palhares, Luis Prado e Paulo Vidigal:

> "Compreende-se que referida hipótese poderia ser suscitada, não somente, mas principalmente, para guarda de dados, mesmo após o término de operações, a serem eventualmente utilizados em procedimento administrativos, judiciais ou arbitrais para constituírem provas de direitos alegados e do cumprimento de obrigações por parte da organização que os maneja" (2021, p. 178)

Como exemplos da utilização desta base legal, tem-se a guarda de informações sobre determinado colaborador, mesmo após sua demissão, durante o prazo prescricional trabalhista. Para casos em que haja ação judicial em curso, haverá possibilidade de retenção dos dados enquanto os fatos ainda estiverem sendo discutidos, desde que os dados pessoais sejam úteis para a finalidade almejada (Lima, 2019, p. 139). Contudo, é essencial que o agente de tratamento utilize tal base legal com boa-fé, evitando o abuso de direito.

Da mesma forma que com as demais bases legais, faz-se essencial a observância dos princípios da lei no momento do tratamento, limitando o tratamento somente aos dados mínimos necessários e adequados à finalidade perseguida. Caso, no mesmo exemplo, o agente de tratamento em sua contestação trabalhista apresente informações que visem difamar o reclamante, sem qualquer relação com o que se discute nos autos, haverá tratamento excessivo e ilegal.

3.2.5 Demais bases legais

Conforme já pontuado no momento em que discutia-se a necessidade de observância das características do agente de tratamento para a correta escolha da base legal, vislumbrou-se que determinadas bases são reservadas exclusivamente

para certos agentes, são elas: a) base legal para a execução de políticas públicas – somente podem ser utilizadas por integrantes da Administração Pública ou entidades vinculadas; b) estudos por órgão de pesquisa – base destinada exclusivamente para órgãos considerados como tal, nos moldes do Art. 5º, XVIII[26]; c) proteção da vida ou incolumidade física do titular – apesar de seu uso não limitar-se a determinado grupo, é notadamente utilizada em casos extremos, assemelhando-se ao estado de necessidade (Art. 188, CC[27]); d) para a tutela de saúde, exclusivamente, em procedimento realizado por profissionais da saúde (exemplos: médicos, enfermeiros, psicólogos, consultórios, etc.) e; e) proteção de crédito – base legal que gera certa discussão, mas que visa a higidez do mercado de crédito (Palhares, Prado e Vidigal, 2021, p. 196), tendo como exemplo perfeito os birôs de crédito.

Ponto que merece ser constantemente reforçado durante todo este trabalho, é o fato de que independentemente da escolha da base legal que irá fundamentar o tratamento, todas elas possuem a mesma força, não havendo de se falar em determinada base legal é mais segura que as demais. O que ocorre é que, para situações específicas, determinadas bases serão adequadas ou não, devendo o agente de tratamento constantemente observar os princípios estabelecidos no art. 6º e a aplicabilidade de cada uma das bases.

Neste diapasão, após a exposição de praticamente todas as bases legais autorizadoras do tratamento de “dados pessoais comuns” e terem sido feitos apontamentos quando o tratamento versar sobre “dados pessoais sensíveis”, há uma base legal que merece aprofundamento em capítulo exclusivo, visto ser considerada uma das bases legais mais polêmicas da lei: o legítimo interesse.

---

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

[27] Art. 188. Não constituem atos ilícitos:
II - a deterioração ou destruição da coisa alheia, ou a lesão a pessoa, a fim de remover perigo iminente.

4. O LEGÍTIMO INTERESSE

Embora haja muita polêmica entorno do legítimo interesse, devido sua aplicação contar com certo grau de subjetividade (Oliveira, 2020, p. 65), não deve o agente de tratamento evitar sua utilização, já que existem na lei outras bases legais mais enigmáticas, como o exercício regular de direito (art. 7, VI), a proteção de crédito (Art. 7, X) ou a prevenção à fraude (Art. 11, II, g), sobre as quais a LGPD sequer dedicou artigo para dar norte interpretativo de referidas bases (Palhares, Prado e Vidigal, 2021, p. 182).

Relembra-se que o rol das bases legais autorizadoras do tratamento de dados pessoais previsto no Art. 7º é exaustivo, não podendo qualquer tratamento ser realizado fora destas hipóteses. Assim, mostrava-se essencial a criação de uma base legal que viesse a dar maior flexibilidade aos agentes de tratamento, o que "não deve ser confundido com uma "carta branca" ou "válvula de escape", de modo a justificar qualquer atividade que seja do interesse do agente de tratamento" (PALHARES, PRADO e VIDIGAL, 2021, p. 182).

Bioni (2019, p. 324) traz o legítimo interesse como uma base mais flexível que as demais, que, embora possua o mesmo nível hierárquico, serviria para que as demais bases legais não fossem "sobrecarregadas". Assim, com a criação do legítimo interesse evitou-se que os agentes de tratamento se vissem obrigados a forçar o enquadramento do tratamento em uma das demais bases legais, que muitas vezes são cabíveis apenas em situações específicas.

Neste viés, importante destacar ponto ainda não abordado neste trabalho, que diz respeito aos fundamentos da disciplina de proteção de dados pessoais, estabelecidos no Art. 2º da LGPD, dentre os quais destaca-se os seguintes:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> **V - o desenvolvimento econômico e tecnológico e a inovação;**
> **VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;** e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Grifo Nosso)

Nota-se que o legislador dentre os 7 (sete) fundamentos elencados pelo artigo, destinou 2 (dois) para versarem sobre a importância do desenvolvimento econômico e da livre iniciativa, sendo imperioso concluir que a LGPD não veio para frear a inovação, muito pelo contrário, mas para regular este avanço sem que fossem

atingidos outros direitos fundamentais. Neste diapasão, é possível compreender toda a lei como um sopesamento entre os fundamentos do art. 2º, onde busca-se garantir os direitos dos titulares sem comprometer a atividade inovativa.

Diferentemente do que ocorre com outros conceitos, não há no Art. 5º definição do que seria o legítimo interesse, devendo a interpretação de tal conceito ser feita de forma literal, onde interesse é aquilo que importa para alguém, enquanto legítimo é adjetivo deste interesse, que deve ser fundamentado pelo bom senso ou pela própria lei (Oliveira, 2020, p. 65). Embora tal conceituação não esteja disposta, a lei trouxe diversas cautelas que devem ser tomadas pelos agentes de tratamento, notadamente as preceituadas no Art. 10º da LGPD (Palhares, Prado e Vidigal, 2021, p.183).

Ainda que não seja o objetivo deste trabalho, a discussão da base legal do consentimento ganhou parágrafos extras por um motivo específico, é a base legal mais fungível com o legítimo interesse. Inclusive, Bruno Bioni (2019, p. 328) já via esta proximidade entre estas bases legais em 2019, ao trazer que “uma das questões mais difíceis será analisar quando a base legal do consentimento seria mais adequada que a do legítimo interesse, e vice-versa”.

Se no consentimento, deixava-se poder exacerbado na mão do titular de dados, com um controle total do tratamento de seus dados pessoais, na base legal do legítimo interesse entende-se que o interesse, muitas vezes comercial, do controlador, é legítimo a ponto de afastar a aplicação das outras bases legais (Palhares, Prado e Vidigal, 2021, p.183).

Como dito anteriormente, não há nada de errado em o interesse do agente de tratamento se resumir ao lucro perseguido. Isso porque, ao verificar os fundamentos dispostos no Art. 2º em conjunto com o Art. 10, I[28], da LGPD, nota-se que o próprio exemplo trazido pelo legislador permite que o agente de tratamento realize o tratamento visando sua expansão comercial, desde que observados os limites impostos pela lei (Oliveira, 2020, p. 74).

Importante destacar que, conforme texto legal, o interesse para ser capaz de fundamentar o tratamento de dados pessoais não necessita ser somente do agente de tratamento, podendo inclusive ser de terceiro. Neste ponto, importante destacar que este “terceiro” não se refere a figura do operador, visto que qualquer tratamento

[28] 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**; (Grifo nosso)

realizado pelo operador em interesse próprio o configurará como controlador de dados, sem prejuízos do possível inadimplemento contratual em que incorrerá frente ao controlador original.

Para exemplificar esta questão, imagine-se que a Empresa A não possua mais justificativas para manter o tratamento de dados de determinado cliente, contudo, descobre que referido cliente está sendo investigado por conta de um escândalo de corrupção, escândalo este que não possui qualquer ligação com os negócios da Empresa A. Deste modo, a empresa terá justificativa para guardar os dados por prazo adicional, pois entende que a autoridade poderá ter interesse no acesso a determinados dados, fundamentando esta guarda no interesse legítimo de terceiro.

Assim, para que o controlador ampare o tratamento no legítimo interesse de terceiro, continua necessário a observância dos princípios da lei, bem como, das balizas de utilização do legítimo interesse, que serão vistas adiante. Além disso, conforme assevera Oliveira (2020, p. 73), o legítimo interesse não pode ser desvirtuado, caso para a consecução do interesse do terceiro seja necessário tão somente o armazenamento dos dados, não poderá o controlador manter um tratamento incompatível com interesse próprio.

Ainda, para balizar a aplicação do legítimo interesse e visando dar maior clareza sobre os limites de aplicação do legítimo interesse, o legislador, no art. 10 da LGPD, elaborou requisitos de observância obrigatória para uma satisfatória aplicação do legítimo interesse. No entanto, antes de adentrar nestes requisitos, importante rememorar que o legítimo interesse não é aplicável para o tratamento de “dados pessoais sensíveis”, de modo que a primeira pergunta que o controlador deve fazer é se existem ou não dados pessoais sensíveis em sua atividade. Se existir, o controlador terá de recorrer para alguma das bases legais previstas no Art. 11 da lei, se não, poderá ser avaliada a utilização do legítimo interesse. Feita esta ressalva, é possível prosseguir no estudo destes requisitos.

4.1 As balizas para a aplicação do legítimo interesse

Na Lei de proteção de dados, há menção ao legítimo interesse em 6 (seis) oportunidades, hora como “legítimo interesse”, em outros momentos como “interesse legítimo”, o que se compreende como pouco comparado a outras bases legais, como a palavra “consentimento”, que aparece 35 (trinta e cinco) vezes.

Embora sejam poucas as aparições, aproveitando-se da história recente, o

Brasil evitou cometer o mesmo erro que a Europa cometeu em sua antiga diretiva (prévia à *GDPR*), em que foi previsto o legítimo interesse sem o detalhamento dos critérios de sua aplicação. Conforme assevera Bioni (2019, p. 325), com este erro, a Europa percebeu que: a) cada país do bloco começou a dar uma interpretação diversa ao legítimo interesse; e b) houve o risco de a aplicação das outras bases ser esvaziado, uma vez que o legítimo interesse sem suas balizas figurava como uma carta em branco.

Desta forma é que o legislador, recorrendo à experiência europeia, definiu as balizas de aplicação do legítimo interesse, sendo possível distribuir tais critérios em: a) finalidades legítimas; b) situações concretas; c) tratamento estritamente do necessário; d) observância da legítima expectativa do titular; e, por fim, e) adoção de medidas para garantir a transparência. Cada um destes pontos será estudado de modo mais aprofundado a seguir.

4.1.1 Finalidades Legítimas

Em seu *caput*, o Art. 10 da LGPD estabelece que “o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas” e, da mesma forma que ocorre com o legítimo interesse, não há definição na lei do que o legislador quis dizer com tal termo, de modo que, é preciso interpretá-lo literalmente. Desta forma, qualquer tratamento realizado com base no legítimo interesse deve respeitar a lei, o bom senso, jurisprudências e demais fontes do direito. Contudo, isso não significa que o interesse perseguido deva estar previsto em lei, mas apenas não pode contrariá-la (Oliveira, 2020, p. 75).

Embora haja previsão expressa no artigo que versa sobre as balizas do legítimo interesse, importante ressaltar que, conforme visto quando tratava-se do princípio da finalidade, o tratamento de dados pessoais com fundamento em qualquer das bases legais não pode ter o condão de contrariar a lei, não sendo este um requisito exclusivo do legítimo interesse.

Assim, é possível entender que o reforço trazido pelo legislador vem no sentido de que, na situação concreta, o bom senso deve prevalecer, indo muito além de situações que violam frontalmente a lei, como, por exemplo, o tratamento de dados pessoais para a comercialização de drogas ilícitas. Em uma situação concreta, um tratamento que embora aparentemente não viole nenhuma lei, pode colocar o titular em posição de risco físico ou psicológico, de modo que será considerado ilegítimo por

este motivo.

É permitido que um agente de tratamento guarde informações sobre todos os vídeos assistidos por determinado titular com base no legítimo interesse? Depende, esta situação somente poderá ser concebida em uma situação concreta, caso este agente seja o Youtube, entende-se que o legítimo interesse está demonstrado, visto que o YouTube é um site que antes de cada vídeo exibe propagandas, sendo assim, quanto mais tempo o usuário permanecer em sua página, mais benéfico para a empresa. Assim, sempre a análise da situação concreta deve prevalecer.

4.1.2 Situações Concretas

Neste viés, a redação do *caput* do artigo 10 segue informando que estas finalidades legítimas deverão ser “consideradas a partir de situações concretas”, de maneira que é possível extrair dois ensinamentos desta indicação: a) a legitimidade do interesse do controlador somente será verificada na situação concreta e; b) o interesse do controlador deve estar fundamentado em uma situação concreta. O primeiro ponto já foi abordado, de modo que o controlador deverá ater-se as especificidades da sua atividade para entender se determinado tratamento é ou não legítimo, indo muito além da mera consulta a lei.

Quanto à necessidade deste tratamento estar fundamentado em uma situação concreta, nota que o legislador buscou impor certa urgência na definição da finalidade do tratamento, de modo que o legítimo interesse não pode ser arguido com base em uma situação futura, prática costumeira das empresas antes do advento da LGPD, devendo o interesse ser, a partir de agora, específico e não especulativo (Oliveira, 2020, p.77).

A necessidade de o interesse do controlador estar fundamentado em uma situação concreta igualmente não é um requisito exclusivo do legítimo interesse, sendo vedado tratamento de dados pessoais sem finalidade definida para que seja possível a observância de diversos princípios, como adequação, necessidade e transparência. O controlador de dados só conseguirá cumprir adequadamente estes princípios se souber qual a situação concreta que pugna pelo tratamento de dados pessoais.

A título exemplificativo, imagine que um comerciante de medicamentos armazene os dados pessoais de todos seus clientes, desde nome, CPF, endereço, até os hábitos de compra em sua loja. Contudo, o faz sem qualquer finalidade imediata,

justificando tal armazenamento no seu legítimo interesse de, possivelmente, no futuro vir a necessitar destes dados. Isto é possível? Não, uma vez que é necessária uma situação concreta específica e não especulativa para a utilização do legítimo interesse.

Embora em um primeiro momento determinados agentes de tratamento possam ter resistência a tal vedação, esta serve inclusive para proteger o mesmo, uma vez que a retenção de dados inúteis apenas expõe o agente de tratamento a riscos desnecessários.

4.1.3 Dados estritamente necessários

Conforme assevera Palhares, Prado e Vidigal (2021, p. 184), independentemente da base legal escolhida, todo agente de tratamento deve fazer a análise do mínimo de dados pessoais necessários para viabilizar a finalidade perseguida, contudo, entende-se que o legislador buscou dar maior destaque a este princípio ao tratar do legítimo interesse, conforme §1 do art. 10:

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

Considerando que o titular de dados é posto em uma situação de maior vulnerabilidade quando o controlador utiliza o legítimo interesse, este reforço imposto pelo legislador traz tranquilidade ao titular, pois garante que não haverá tratamento excessivo de seus dados pessoais.

A reflexão que deve ser feita sempre é: a finalidade almejada poderia ser alcançada com menos dados pessoais? Se sim, o tratamento deve ser revisto. Sobre este ponto, importante apropriar-se do didático exemplo trazido por Bruno Bioni (2019, p. 331) versando sobre as relações de trabalho: considerando o monitoramento do tráfego da rede corporativa, o quão desnecessariamente intrusivo é o monitoramento constante, inclusive com a utilização de *keyloggers*[29]? Não seria possível alcançar o fim almejado apenas bloqueando *sites* que conhecidamente limitam a produtividade dos funcionários? Estas são as reflexões que devem ser feitas para a adequada utilização do legítimo interesse.

[29] Key-logger é um dispositivo, *software* ou *hardware, capaz de* capturar todos os caracteres digitados pelo usuário.

4.1.4 Legítima Expectativa do Titular

Ao referir o legítimo interesse, alguns contornos de seu significado podem ser encontrados na lei, contudo, a “legítima expectativa” é mencionada unicamente no inciso II do Art. 10, momento em que o legislador discorre sobre o rol exemplificativo de hipóteses em que o legítimo interesse pode ser utilizado.

> 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. (Grifo nosso)

Porém, novamente a interpretação literal não falha, sendo possível compreender a legítima expectativa como uma extensão da boa-fé. Neste diapasão, Oliveira (2020, p. 119) expõe que a legítima expectativa possui ampla conexão com o princípio da confiança, que possui como escopo a defesa das legítimas expectativas que nascem entre as partes de um contrato.

A legítima expectativa torna-se mais compreensível a partir de exemplos, assim, suponha-se que João compre todos os dias carne no mesmo mercado, informando seu CPF para desconto no IPVA. Diante deste compartilhamento, algumas ações por parte do mercado são esperadas, como o envio da nota fiscal ao ente estadual para que recebimento do desconto no IPVA, bem como, é possível que o mercado analise seu consumo. Contudo, já não está na expectativa de João que seus dados sejam compartilhados com terceiros alheios ao mercado, ou ainda, que ele receba um *mailing* uma vez que sequer informou seu endereço eletrônico.

Trazendo para o ambiente digital, um outro exemplo de utilização do legítimo interesse é a sugestão de vídeos similares aos assistidos dentro de uma mesma plataforma. Ora, principalmente com serviços gratuitos, os dados pessoais são utilizados como pagamento, principalmente para a realização de publicidade comportamental. Assim, é um legítimo interesse do controlador que o usuário passe mais tempo dentro da plataforma de vídeos, motivo pelo qual estas plataformas sugerem vídeos de interesse do titular. Neste caso, o tratamento de dados pessoais é benéfico para ambas as partes, uma vez que a plataforma de *streaming* de vídeos ganhará mais dinheiro com propagandas, enquanto o usuário verá conteúdos que lhe interessam. O mesmo não pode ser dito caso as preferências de visualização de determinado usuário fossem compartilhadas individualizadas em alguma pesquisa, o que com certeza surpreenderia o titular dos dados e acarretaria problemas ao

controlador.

Da mesma maneira que só será possível concluir se a finalidade do controlador é legítima ou não a partir de uma situação concreta, a legítima expectativa igualmente necessita ser analisada dentro de um contexto. Embora para definição de legítima expectativa sempre há de se considerar o “homem médio”, aquele que pensa de acordo com determinada coletividade, é necessário ver que este contexto também é mutável:

> Obviamente, a Legítima Expectativa varia de contextos sociais e históricos. A sensibilidade quanto à invasão de privacidade de 30 anos atrás é muito diferente dos dias atuais. Nossa sociedade conectada vem “trocando” dados por “funcionalidades” e, mesmo que se pudesse condicionar a aquisição de um determinado produto ou serviço a uma verdadeira devassa da privacidade e intimidade, ainda assim grande parte da sociedade se submeter, como podemos ver com o número sempre crescente de pessoas que utilizam redes sociais. (OLIVEIRA e COTS, 2020, p. 93)

Embora em ambos exemplos haja uma relação prévia entre o titular dos dados pessoais e o controlador de dados, este não é um requisito para a utilização do legítimo interesse. Certo é, que a prévia relação entre o titular e o controlador apenas fortalece as justificativas para utilização desta base legal, o que não se confunde com uma exigência legal (Palhares, Prado e Vidigal, 2021, p. 185). Discorrendo sobre a legítima expectativa do titular, Bruno Bioni (2019, p. 328) demonstra a ligação deste requisito ao princípio da finalidade, onde o uso superveniente tem de ser compatível com aquele que originou a coleta.

Quando uma pessoa adquire um veículo de uma revendedora, não será tão surpreendente que após alguns dias, um despachante ligue para falar sobre o emplacamento do mesmo, ainda, que poucos dias adiante uma corretora envie uma proposta de seguro veicular. Veja-se que em ambas situações o titular só possuía relação direta com a concessionária que vendeu o veículo, contudo, estaria dentro das expectativas de um homem médio a oferta de serviços adicionais (Oliveira, 2021, p. 92).

Embora alguns exemplos tenham sido expostos para facilitar a compreensão do legítimo interesse e da necessidade do tratamento estar dentro das legítimas expectativas do titular, tais situações não devem ser compreendidas como verdades absolutas, pois sempre será necessário analisar o contexto da atividade do controlador e o tipo de dados envolvidos.

4.1.5 Transparência e *opt-out*

Por fim, a LGPD estabelece que “o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse”. Novamente, a Lei não inova ao trazer a transparência como um requisito para a utilização do legítimo interesse, uma vez que a transparência deverá ser observada em qualquer tratamento de dados pessoais, independentemente da base legal escolhida.

Entretanto, da mesma forma que o princípio da necessidade é reafirmado no Art. 10, entende-se que o legislador buscou reforçar a necessidade de cumprimento do princípio da transparência mesmo quando o tratamento for baseado no legítimo interesse. Esta foi a forma encontrada de balancear a relação entre o controlador e o titular dos dados, “de modo a fazer contrapeso ao baixo grau de autonomia dele (titular) em relação à ocorrência ou não de tal atividade” (PALHARES, PRADO e VIDIGAL, p. 185), uma vez que o legítimo interesse não pressupõe autorização do titular.

Bruno Bioni (2019, p. 329) destaca que a transparência se faz necessária principalmente para viabilizar o direito do titular de opor-se ao tratamento (*opt-out),* notadamente quando considerar que o tratamento está fora de sua legítima expectativa. Por vezes, o direito de opor-se ao tratamento será feito em forma de questionamentos e solicitação de melhoria no processo, uma vez que vedar o tratamento por completo não será uma opção, como é o caso de um funcionário que se recuse a ser filmado na entrada do seu emprego. Com a ciência de que está sendo filmado, o funcionário poderá solicitar maiores esclarecimentos sobre o armazenamento, tratamento, finalidades e sugerir melhorias, de modo que caso inexistisse a transparência, o titular acabaria com dificuldades de exercer seus demais direitos.

Depreende-se que embora o legislador tenha estabelecido expressamente diversas balizas para a utilização do legítimo interesse, não o fez para adicionar entraves na sua utilização, uma vez que não se tratam de requisitos exclusivos desta base legal. Com os destaques estabelecidos no art. 10, o legislador conseguiu chamar atenção para determinados princípios e ao mesmo passo evitou que a interpretação do legítimo interesse fosse guiada meramente pela subjetividade do interesse do controlador, evocando a importância do titular dos dados nesta relação.

4.2 Documentos para a utilização do legítimo interesse

Como mencionado alhures, a LGPD não busca ser uma lei proibitiva e sancionatória, mas sim uma lei principiológica, de modo que a análise de adequação não é binária, ou seja, não existe apenas estar ou não adequado, mas sim estar melhor ou pior adequado. O que se busca demonstrar é que somente a soma de boas práticas demonstrará a conformidade de um agente de tratamento. Mas como demonstrar esta conformidade? Existem diversos modos, como um site com avisos de privacidade, uma detalhada política de privacidade acessível, o armazenamento do consentimento do titular, dentre uma infinidade de documentos, onde o que importa é demonstrar a seriedade e cautela do agente de tratamento frente aos dados pessoais que lhe foram confiados.

Apesar de existirem diversos meios de estar em conformidade com a lei, visando estabelecer um padrão, o legislador, buscando diretamente na fonte europeia, determinou documentos essenciais para apresentação à ANPD, conforme se verá a seguir. Apesar disso, considerando a temática do presente trabalho, dar-se-á ênfase no primeiro momento a um documento que não está previsto na LGPD, o LIA (*Legitimate Interest Assessment)* ou como é chamado pelos operadores da lei: o teste de ponderação do legítimo interesse.

4.2.1 *Legitimate Interest Assessment* – Teste de ponderação do legítimo interesse

Embora não haja previsão específica quanto a necessidade de elaboração deste documento na lei brasileira, sua utilização auxiliará o controlador de dados tanto no momento da escolha da base legal quanto na hora de demonstrar sua conformidade com a lei. O *LIA* consiste na documentação da avaliação das balizas anteriormente ensinadas que, conforme assevera (Palhares, Prado e Vidigal, 2021, p. 186), podem ser resumidas da seguinte forma: a) verificação da ausência de dados sensíveis; b) verificação da legitimidade do interesse na situação concreta; c) verificação da estrita necessidade; e d) verificação da transparência e expectativa do titular.

Outros autores como Bioni (2019, p. 328) e Oliveira (2020, p. 101) trazem parâmetros ligeiramente diferentes, elencando como critérios a análise da legitimidade do interesse do autor, em um sentido de legalidade, e a impossibilidade de o legítimo interesse violar direitos fundamentais. Contudo, conforme relembra Palhares, Prado e

Vidigal (2021, p. 187) após apresentar seu modelo, tanto a legitimidade do fim perseguido, como a impossibilidade de o tratamento atingir liberdades fundamentais do titular é inerente a todas as bases legais, de modo que não se trata de avaliação da aplicabilidade do legítimo interesse, mas sim de uma avaliação de legalidade do tratamento, independentemente da base que fundamenta o tratamento.

Ponto polêmico e que gera discussões, não somente no LIA, mas em todos documentos que porventura possam ser exigidos pela ANPD, é a necessidade de elaboração prévia destes documentos ou não. Para Palhares, Prado e Vidigal (2021, p. 188), o LIA não é obrigatório para qualquer tratamento, mas sim um meio de provar a conformidade que deve ser utilizado com parcimônia, sob pena de burocratizar demasiadamente o trabalho dos operadores da lei, tornando o trabalho operacional, repetitivo e pouco estratégico, uma vez que serão elaborados diversos "relatórios de gaveta", que jamais serão utilizados.

Bioni (2019, p. 327) por sua vez afirma que embora não previsto expressamente, o uso do legítimo interesse passa por uma análise sistemática dos arts. 6º, X, 10 e 37, devendo o teste de proporcionalidade ser documentado. Como mencionado, não há previsão expressa na lei brasileira quanto a necessidade de elaboração de um LIA, o que existe no art. 10, §3, é o comando para a elaboração de um outro documento, que será estudado adiante. Sobre o artigo e a obrigatoriedade do LIA, acentua Luis Fernando Prado[30]:

> (...) faz menção expressa ao RIPD (ainda que isso não signifique, a meu ver, que o mero enquadramento de uma atividade no LI demande a realização de RIPD). De qualquer forma, entre RIPD e LIA, sugere-se que os agentes de tratamento concentrem seus esforços na elaboração do primeiro, pois, de outra forma, há risco de que os LIAs que atualmente vêm sendo elaborados em larga escala pelos agentes de tratamento gerem o retrabalho de serem substituídos por RIPDs quando houver eventual requisição da ANPD. Isso porque, ao contrário do LIA, o RIPD é um documento expressamente previsto na LGPD, com conteúdo (minimamente) definido (art. 5º, XVII), que poderá ser objeto de requisição específica pela autoridade.

Assim, entende-se que existem outros mecanismos aptos a demonstrar que o agente de tratamento tomou as devidas providências para a utilização do legítimo interesse, como, por exemplo, troca de e-mails, consulta de especialistas, mecanismos de transparência, dentre outros. Entretanto, conforme mencionado por Luis Prado acima, existe outro documento que poderá vir a ser solicitado pela ANPD

[30] LGPDRIVE. Disponível em <https://www.lgpdrive.com.br/cap-ii-art-7%C2BA-16#h.xgh8486mmfb5> Acessado em 12 de set de 2021.

e que encontra correspondência na lei, o RIPD.

4.2.2 Relatório de Impacto à Proteção de Dados (RIPD)

Diferentemente do que ocorre com o LIA, o Relatório de Impacto à Proteção de Dados (RIPD) é um documento que encontra correspondência na LGPD, inclusive sendo conceituado à luz do artigo 5º como a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos".

Não obstante, é previsto que a ANPD poderá solicitar referida documentação em dois casos, são eles:

> Art. 10 § 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.
>
> 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. (Grifo Nosso)

O RIPD pode ser compreendido como um documento que auxiliará o controlador de dados a analisar, identificar e minimizar os riscos inerentes ao tratamento de dados pessoas. Pode ser entendida como parte essencial de sua obrigação e que, quando feito de forma adequada, servirá de auxílio para avaliar e demonstrar sua própria conformidade com suas obrigações de proteção de dados.

Capanema (2019, p. 292) traz analogia didática, afirmando que a finalidade do RIPD é muito similar ao do EIA[31]/RIMA[32] do Direito Ambiental, documentos estes que avaliam os impactos que determinado empreendimento poderá causar ao meio ambiente, bem como, seu um plano para mitigação destes riscos.

Considerando que a ANPD ainda não providenciou modelo ou orientação no sentido de elaboração do RIPD, os profissionais de proteção de dados possuem somente o texto legislativo, motivo pelo qual vêm utilizando modelos fornecidos

[31] Estudo de Impacto Ambiental
[32] Relatório de Impacto ao Meio Ambiente

internacionalmente, como é o caso da agência nacional britânica, a ICO – *Information Commissioner's Officer*, que elaborou lista de requisitos para a versão europeia do RIPD (DPIA): a) identificar qual é objeto do projeto e quais as espécies de tratamento relacionadas; b) como é feito o tratamento de dados – como são coletados? Quais suas origens? São compartilhados? c) Quais os tipos de tratamento que oferecem maior risco/ Como evitá-los ou mitiga-los? d) Há dados de crianças e adolescentes; e) Quais as finalidades dos tratamentos; e f) quais os fundamentos dos tratamentos.

Porém, qual é o momento de elaboração do RIPD? Felipe Palhares, em 2019 em obra de coordenação de Viviane Maldonado (p. 280) ressalta que por se tratar de ferramenta apta a identificar riscos à privacidade de determinado projeto, o RIPD deve ser idealmente elaborado a partir do projeto, ou tão logo seja viável. Embora ideal, verificar-se-á que não é obrigação do controlador de dados elaborar referido relatório previamente ao tratamento, inclusive é o que se extrai das próprias palavras do legislador no projeto de lei que originou a LGPD. Assevera o Deputado Federal Orlando Silva[33]:

> Entendemos que a elaboração de relatórios de impacto à proteção de dados é uma atividade benéfica no gerenciamento do negócio pelo próprio responsável. A elaboração permite uma reflexão sobre os procedimentos adotados e contribui para a identificação de eventuais falhas, mitigando a possibilidade de danos antes mesmo que estes ocorram. **Assim, a elaboração prévia por motivações próprias é extremamente salutar para os agentes de tratamento. Entretanto, entendemos que esta deve ser uma decisão dos próprios agentes e não uma imposição da burocracia**. (Grifo Nosso)

É o que se extrai inclusive da redação do art. 38, que indica que a "autoridade nacional poderá determinar ao controlador que elabore relatório", não indicando em nenhum momento que o mesmo deva estar pronto. Não seria factível que para todos os tratamentos realizados por uma empresa fosse necessário a elaboração de um documento, sob perigo de que a lei fracassasse.

Muito embora haja mudança ortográfica no artigo que versa sobre referido relatório no momento em que se trata do legítimo interesse (Art. 10, §3), entende Palhares, Prado e Vidigal (2021, p. 190) que o tratamento deva ser o mesmo, ou seja, não há necessidade de o relatório estar previamente pronto, apesar de ser considerado uma boa prática. Assim, onde legislador indica que é a autoridade

---

[33] Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=> Acessado em: 12 de set. de 2021.

nacional que “poderá solicitar”, entende-se que deveria estar presente também a palavra “elaborar”, de modo que a escolha do legítimo interesse não acarreta em ônus burocrático ao agente de tratamento. Caso não foste este o entendimento, deveria o legislador, pelo princípio da legalidade, indicar que a simples ausência de RIPD acarretaria a violação à lei, o que não fez.

Assim, constata-se que as documentações especificadas para análise do legítimo interesse servem mais para auxiliar o agente de tratamento do que para lhe impor encargo, de modo que o agente disporá de documentos extras para a demonstração de sua conformidade.

5. CONCLUSÃO

Conforme visto no presente trabalho, vive-se em um mundo em que o processamento de dados pessoais é realizado de forma ininterrupta por diversos agentes do mercado, estes que buscam, a partir deste tratamento, obter vantagens competitivas frente a seus concorrentes. Durante muito tempo o direito à privacidade consignado no art. 5º, X, da Constituição Federal foi suficiente para resguardar o titular dos dados de tratamentos abusivos, contudo, quando os interesses do mercado começaram a conflitar com os direitos fundamentais dos indivíduos, a sociedade suplicou por uma lei específica para tratar sobre o tema.

Fazendo uma analogia com o mundo computacional, quando um site apresenta problemas, prontamente um programador é acionado para entrar em ação, corrigindo este defeito e, muitas vezes, implementando uma melhoria. Com a sociedade não é diferente, após o escândalo de divulgação de documentos por parte do ex-agente da CIA, Edward Snowden, o legislador, representante da sociedade, apressou-se para aprovar uma solução apta a evitar que os dados que transitam na internet carecessem de regulamentação, promulgando o Marco Civil da Internet - MCI.

Com avanço mundial das discussões acerca de privacidade pelo mundo, a Europa, berço das discussões sobre privacidade do mundo moderno, editou a GDPR, impondo diversas condições àqueles que desejassem negociar com empresas lotadas no velho continente. Muito embora o MCI contivesse um microssistema de proteção de dados pessoais, este era insuficiente, uma vez que sua aplicabilidade se restringia ao ambiente virtual, mais especificamente, à internet.

Neste contexto é editada a LGPD - Lei Geral de Proteção de Dados Pessoais, norma brasileira apta a regular o tratamento de dados pessoais em território brasileiro, ou ainda, o tratamento de dados pessoais de brasileiros no exterior. A lei, de maneira acertada, ao invés de engessar seu texto indicando o que seria permitido ou não em sede de tratamento de dados pessoais, estabeleceu os princípios que devem ser observados pelos agentes de tratamento, de modo a perseverar sua efetividade no tempo.

No primeiro capítulo, após introduzidos conceitos básicos para compreensão de legislação, aprofundou-se nestas balizas da lei, mais especificamente naqueles princípios que outrora seriam úteis para a compreensão do legítimo interesse. Além disso, demonstrou-se que a observância dos princípios é obrigatória, independentemente da base legal escolhida para embasar o tratamento dos dados

pessoais.

No segundo capítulo foi verificada a emancipação do consentimento, única base legal capaz de fundamentar o tratamento de dados pessoais no MCI. Com o advento da LGPD, outras bases legais foram positivadas, sendo colocadas lado a lado com o consentimento, eliminando qualquer hierarquia que pudesse existir entre elas.

Igualmente constatou-se a importância da correta definição da base legal que, se feita da maneira adequada, iluminará o caminho do agente de tratamento quanto ao respeito aos princípios e aos direitos dos titulares. Para as principais bases legais dedicou-se subcapítulo exclusivo, com ênfase no consentimento, por ser a base legal mais fungível com a do legítimo interesse.

Já no terceiro e último capítulo, introduziu-se a base legal objeto deste trabalho: o legítimo interesse. Com o estudo, verifica-se que a existência do legítimo interesse anda ao lado dos fundamentos econômicos da LGPD, uma vez que se trata de uma das bases legais mais flexíveis, evitando que a lei se tornasse um entrave para a inovação e à livre iniciativa.

Apesar de mais flexível, o legítimo interesse teve a devida atenção do legislador, que no art. 10 trouxe exemplos da utilização do legítimo interesse e estabeleceu os limites para a sua utilização. Apesar de os critérios estabelecidos serem muito similares aos princípios da LGPD, notadamente o princípio da finalidade, adequação, necessidade e transparência, sua repetição ajuda a compreender a atenção que o agente de tratamento deve ter ao tratar dados pessoais baseado meramente em seu interesse.

Considerando que na prática do profissional de proteção de dados o legítimo interesse será muitas vezes a base legal apta a fundamentar o tratamento de dados pessoais, faz-se imprescindível a compreensão dos testes que podem ser realizados a fim de verificar se o legítimo interesse foi devidamente empregado, bem como, a documentação que auxiliará na demonstração da conformidade do agente de tratamento.

Neste viés, debruçou-se sobre dois documentos específicos: a) o LIA (Legitimate Interest Assessment), documento importado pela doutrina do regramento europeu, mais especificamente da opinião do WP29, que objetiva um teste de ponderação para utilização do legítimo interesse; e b) o RIPD – Relatório de Impacto à Proteção de Dados, este previsto em nossa lei que poderá vir a ser solicitado ao controlador dos dados pela agência reguladora, que deverá conter informações sobre

o tratamento. Embora a elaboração prévia de ambos documentos auxilie na comprovação da conformidade do agente de tratamento, demonstrou-se que tais documentos não precisam estar prontos no momento da solicitação da ANPD, sendo crível que será disponibilizado tempo para entrega destes.

Por todo o exposto, conclui-se que o legítimo interesse, embora mais flexível que as demais bases legais, não goza de menor força, tendo a mesma rigidez que qualquer outra base legal, desde que empregado da maneira adequada. Ainda, verifica-se que o legislador fez questão de demonstrar que o legítimo interesse não é uma carta em branco para justificar todo e qualquer tratamento de dados pessoais, reforçando que para utilização desta base legal a observância dos princípios continua obrigatória, inclusive destacando alguns que merecem especial atenção.

Por fim, conclui-se que com tais balizas e documentações o legislador em nenhuma hipótese buscou dificultar a utilização do legítimo interesse, mas prover meio de o agente de tratamento provar sua conformidade. A utilização de qualquer das bases legais exporá o agente de tratamento a algum risco, contudo, evitar a utilização do legítimo interesse poderá ser fatal para um programa de privacidade de dados.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ARTICLE 29 WORKING PARTY: Opinion 03/2013 on purpose limitation. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> Acesso em 29 de ago. 2021

ARTICLE 29 WORKING PARTY. Guidelines on consente under Regulation 2016/679. Disponível em: < https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> Acesso em: 04 de set de 2021.

ARTICLE 29 WORKING PARTY. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en> Acesso em 07 de set. 2021

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BORELLI, Alessandra et. al. LGPD: Lei Geral de Proteção de Dados comentada/coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. --2. ed. -- São Paulo : Thomson Reuters Brasil, 2019

BRASIL. Constituição da República Federativa do Brasil. Promulgada em 05 de outubro de 1988. Disponível em :<http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>.

BRASIL. Lei Geral de Proteção de Dados Pessoais. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

BRASIL. Marco Civil da Internet. Lei n. 12.414, de 9 de junho de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

CAPANEMA, Walter. Elaboração e Revisão de Documentos. In: MALDONADO, Viviane (coord.). LGPD Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. 5. ed. São Paulo: Thomson Reuters, 2019. cap. 8, p. 303-326. ISBN 978-85-5321-825-7.

CRUZ, Andresa et al. O LEGÍTIMO INTERESE E A LGPD: Lei Geral de Proteção de Dados Pessoais. / Ricardo Oliveira, Márcio Cots, coordenação. -- 2ª . ed. São Paulo:

Thomson Reuters, 2020. 311 p. ISBN 978-85-5065-177-0

DE LIMA, Adriano Carlos et al. LGPD Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. / Viviane Nóbrega Maldonado, coordenação -- 5ª . ed. São Paulo: Thomson Reuters, 2019. 368 p. ISBN 978-85-5321-825-7.
DONEDA, Danilo. Princípios de Proteção de Dados Pessoais. In: LUCCA, Newton de; SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). Direito & Internet III: Marco civil de internet. Quartier Latin, 2015.

LEONARDI, Marcel. Aspectos controvertidos entre a Lei Geral de Proteção de Dados e o Marco Civil da Internet. Temas Atuais de Proteção de Dados. / Felipe Palhares, coordenação --. São Paulo: Thomson Reuters Brasil, 2020.

MALDONADO, Viviane. A Lei Geral de Proteção de Dados: objeto, âmbito de aplicação, requisitos, segurança e a necessidade de sua correta implementação. In: MALDONADO, Viviane (coord.). LGPD Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. 5. ed. São Paulo: Thomson Reuters, 2019. Introdução, p. 11-34. ISBN 978-85-5321-825-7.

PALHARES, Felipe; PRADO, Luis; VIDIGAL, Paulo. COMPLIANCE DIGITAL E LGPD. 1ª . ed. Brasil: Thomson Reuters, 2021. 399 p. v. V. ISBN 978-65-5614-605-8.

PALHARES, Felipe. O Relatório de Impacto à Proteção de Dados Pessoais. In: MALDONADO, Viviane (coord.). LGPD Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. 5. ed. São Paulo: Thomson Reuters, 2019. cap. 7, p. 261-302. ISBN 978-85-5321-825-7.

SILVA, De Plácido. Vocabulário Jurídico. 18 ed. Rio de Janeiro: Forense, 2001.

WARREN, Samuel; BRENDEIS, Louis. Harvard Law Review, v. 4, n. 5. 15 de dezembro de 1890.