FUNDAÇÃO DE ENSINO “EURÍPIDES SOARES DA ROCHA” – FEESR
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM DIREITO – PPGD
MESTRADO EM DIREITO

Jéssica Cabrera Reis

O ENCARREGADO DE PROTEÇÃO DE DADOS NA LEI GERAL DE PROTEÇÃO DE DADOS SOB O PARADIGMA DA *GENERAL DATA PROTECTION REGULATION*

Marília, SP
2020

Jéssica Cabrera Reis

O ENCARREGADO DE PROTEÇÃO DE DADOS NA LEI GERAL DE PROTEÇÃO DE DADOS SOB O PARADIGMA DA *GENERAL DATA PROTECTION REGULATION*

Dissertação apresentada ao Programa de Pós-graduação *Stricto Sensu* – Mestrado em Direito – do Centro Universitário Eurípides de Marília – UNIVEM, em sua Área de Concentração em Teoria do Direito e do Estado, Linha de Pesquisa Construção do Saber Jurídico, como requisito à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Mário Furlaneto Neto

Marília, SP

2020

Dedicado aos Santos da Silva e aos Cabrera,
que ficaram com o sobrenome ou não
e aí, aos que os têm no sangue e também no coração
a todos vocês, responsáveis por ser quem eu sou que são!

AGRADECIMENTOS

Gratidão ao Prof. Dr. Mário Furlaneto Neto, por se propor ao desafio de me orientar em pesquisa proposta já na reta final, por toda a dedicação, paciência e incentivo, fundamentais a qualquer orientando.

Ricardo Maravalhas, amigo, sócio, mentor, irmão e às vezes também pai. Obrigada por ter se colocado em meu caminho, por toda a paciência, resiliência e apoio incondicionais.

Sócios e amigos da Maravalhas Legal: muito obrigada pela paciência e apoio constantes. Melhor que ter colegas de trabalho é quando eles são uma verdadeira família, como são vocês.

Obrigada a todos os meus amigos. Como poderia enumerá-los? Impossível. Espalhados em todo este Brasil, e também fora dele, a todos vocês meu muito obrigada, sobretudo por me colocarem nos trilhos nos momentos em que meus vagões se descarrilham... Vocês são força para alcançar meus objetivos!

Aos Lima e aos Garcia, minha eterna gratidão pelo acolhimento de sempre, a força e os sorrisos cotidianos com os quais me contemplam. Vocês já são parte inseparável de quem eu sou, e sou muito melhor perto de vocês.

Stephanie Garcia, saiba da minha eterna gratidão pelo seu amor de sempre, pelo crescimento constante que nos proporcionamos a cada dia, pelo apoio genuíno e pela nossa parceria imbatível. Gratidão por me ensinar o significado de gratidão, podendo ser verdadeiramente grata a todos aqui mencionados, inclusive você.

RESUMO

Visa-se analisar a figura do encarregado de proteção de dados pessoais concebido pela Lei Geral de Proteção de Dados sob o paradigma da *General Data Protection Regulation*. O estudo é realizado sob a linha de pesquisa Construção do Saber Jurídico, do Programa de Pós-Graduação em Direito. Utiliza-se o método dedutivo e a revisão bibliográfica, consubstanciada em análise da literatura jurídica e da legislação, brasileira e da União Europeia. Para tanto, examina-se o contexto econômico e jurídico em que se insere a proteção de dados pessoais. Após, aborda-se os temas essenciais da Lei Geral de Proteção de Dados para compreensão do encarregado de proteção de dados. Por fim, se analisa ponto a ponto as diversas temáticas que emolduram a figura do encarregado de proteção de dados, comparando-se as disposições da Lei Geral de Proteção de Dados com as da *General Data Protection Regulation* sobre o *data protection officer*. Conclui-se que as funções do *data protection officer* na Lei Geral de Proteção de Dados são equivalentes às da *General Data Protection Regulation*. Além disso, o *data protection officer* pode ser pessoa natural ou jurídica, que atua interna ou externamente na organização. Em seguida, conclui-se que o *data protection officer* precisa ter conhecimento em Direito sobre proteção de dados pessoais, com capacidade para exercício de suas funções, a despeito de não lhe ser exigida uma formação específica em determinada área. Demais, haverá conflito de interesses entre o exercício da função de *data protection officer* em favor de uma organização para a qual preste outros serviços se nestas atividades houver decisão sobre finalidades e meios de tratamento de dados pessoais. Por outro lado, o conflito de interesses entre o advogado que preste serviços à organização e o exercício da função de *data protection officer* é indissociável, porque os objetivos das funções são díspares. É obrigatória a designação de *data protection officer* pelo controlador, mas àquele que não estiver obrigado, caso o indique, deverá observar o mesmo regime jurídico aplicável ao *data protection officer* obrigatório. Outrossim, a não obrigatoriedade da indicação do *data protection officer* não dispensa a observância da Lei Geral de Proteção de Dados. Conclui-se, também, que o *data protection officer* pode ser uma consultoria externa especializada, podendo ser compartilhado entre diversos agentes de tratamento. Além do mais, conclui-se que o *data protection officer* tem autonomia para funcionar em busca do cumprimento do regime jurídico de proteção de dados pessoais, e, nesse sentido, a documentação dos seus atos, obrigatória, auxilia a preservação dessa autonomia. Por fim, sobre a responsabilidade civil, conclui-se ser o agente de tratamento responsável direto perante a Autoridade Nacional de Proteção de Dados e os titulares de dados, bem como por eventual violação de normas sobre proteção de dados pessoais, a caber ao agente de tratamento regressar em face do *data protection officer*, conforme a relação jurídica que este mantenha com a organização, caso haja praticado ilícito em suas funções. E no caso da responsabilidade do ponto de vista penal, será o *data protection officer* responsável na hipótese em que efetivamente tenha dado causa a eventual violação de bem jurídico protegido por norma penal.

Palavras-chave: privacidade; proteção de dados pessoais; encarregado de proteção de dados pessoais.

ABSTRACT

The research aims to analyse the figure of the personal data protection officer conceived by the brazilian *Lei Geral de Proteção de Dados* under the General Data Protection Regulation paradigm. The study is carried out under the research line Construction of Legal Knowledge, of the Postgraduate Law Program. The deductive method and the bibliographic review are used, consisting of an analysis of the Brazilian and European Union legal literature and legislation. To this end, the economic and legal context in which the protection of personal data is inserted is examined. Then, the essential themes of the brazilian *Lei Geral de Proteção de Dados* are addressed for the data protection officer's understanding. Finally, the various issues surrounding the data protection officer are analyzed from point to point, comparing the provisions of the brazilian *Lei Geral de Proteção de Dados* with those of the General Data Protection Regulation on data protection officers. It is concluded that the functions of the data protection officer in the brazilian *Lei Geral de Proteção de Dados* are equivalent to those of the General Data Protection Regulation. In addition, the data protection officer may be a natural or legal person, acting either internally or externally within the organisation. It is then concluded that the data protection officer must have knowledge of personal data protection law, with the ability to perform his or her duties, even if he or she does not have specific training in a particular area. Moreover, there will be a conflict of interest between the exercise of the data protection officer's function in favor of an organisation for which he or she provides other services if in these activities there is a decision on purposes and means of processing personal data. On the other hand, the conflict of interest between the lawyer providing services to the organisation and the exercise of the data protection officer function is inseparable, because the objectives of the functions are different. The designation of a data protection officer by the controller is mandatory, but those who are not obliged to do so, if they so indicate, must observe the same legal regime applicable to the mandatory data protection officer. In addition, the fact that the data protection officer is not obligatory does not dispense the organization is compliance with the brazilian *Lei Geral de Proteção de Dados*. It is also concluded that the data protection officer may be a specialized external consultancy, which may be shared among several processing agents. Furthermore, it is concluded that the data protection officer has the autonomy to operate in pursuit of compliance with the legal regime of personal data protection, and, in this sense, the documentation of its acts, mandatory, helps preserve this autonomy. Finally, about civil liability, it is concluded that the treatment agent is directly liable to the National Data Protection Authority and the data subjects, as well as for any violation of personal data protection regulations, and that the treatment agent must return to the data protection officer, according to the legal relationship the data protection officer maintains with the organization, in the event it has committed unlawful acts in its functions. And in the case of criminal liability, the data protection officer shall be liable in the event that he or she has actually given rise to a possible violation of a legal property protected by criminal law.

Keywords: privacy; personal data protection; data protection officer.

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

Art. – Artigo

CDC – Código de Defesa do Consumidor

CEDOAB – Código de Ética e Disciplina da Ordem dos Advogados do Brasil

CEO – *Chief executive officer*

CF – Constituição Federal

CLT – Consolidação das Leis do Trabalho

CP – Código Penal

DPO – *Data protection officer* ou *data privacy officer*

EAOAB – Estatuto da Advocacia e da Ordem dos Advogados do Brasil

EPD – Encarregado de proteção de dados

GDPR – *General Data Protection Regulation*

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

SUMÁRIO

1 INTRODUÇÃO

A presente pesquisa visa analisar as nuances afeitas ao encarregado de proteção de dados pessoais, instituído pela LGPD (Lei Geral de Proteção de Dados Pessoais), sob o paradigma da GDPR (*General Data Protection Regulation*), a trazer-se, assim, elementos comparativos para elaborar ao final uma moldura da atuação (em sentido amplo) do DPO (*data protection officer*) no Brasil, especificamente nas organizações privadas.

Para fazê-lo, utiliza-se o método de pesquisa dedutivo, desenvolvido sob o procedimento metodológico de análise bibliográfica da literatura jurídica e da legislação brasileira e da União Europeia.

A pesquisa, assim, é dirigida sob a linha de pesquisa Construção do Saber Jurídico, do Programa de Pós-Graduação em Direito.

O tema é de expressiva relevância, dado que, a despeito de no sistema jurídico brasileiro ter-se concebido algumas disposições para a proteção dos dados pessoais, em especial o *habeas corpus* na Constituição Federal, e disposições sobre o tema no Código de Defesa do Consumidor, na Lei de Acesso à Informação e no Marco Civil da Internet, ainda se demandava um sistema jurídico organizado e completo de proteção aos dados pessoais.

Tal demanda foi mais fortemente impulsionada pela concepção da *General Data Protection Regulation*, cujo vigor iniciou em 2018 e, ante as suas disposições, praticamente obrigou que países que pretendessem manter as relações comerciais com os países membros da União Europeia, concebessem um sistema de proteção de dados pessoais em equivalência com a proteção conferida pela GDPR.

E, nesse sentido, foi publicada a LGPD, Lei 13.709 de 14 de agosto de 2018, a qual estabeleceu, em seu Art. 41, a figura do *data protection officer*, ou encarregado pelo tratamento de dados pessoais, cujo papel se fixou como fundamental à aplicação efetiva da LGPD, todavia, a despeito disso, sem que tenha a Lei especificado diversos temas que levantam questionamentos sobre a figura do DPO.

Assim, como objetivo geral, se pretende analisar os diversos aspectos jurídicos que envolvem o encarregado de proteção de dados pessoais como concebido na LGPD, e, assim, afixar conclusões sobre essas diversas nuances em comparação com as disposições da GDPR também concernentes ao DPO.

Como objetivos específicos, primeiro se analisa o contexto em que é concebida a LGPD, de forma a se abordar a economia da informação, o surgimento

do direito à privacidade, e o seu consectário direito à proteção de dados pessoais, a analisar-se, nesse sentido, as primeiras legislações e institucionalizações de sistemas jurídicos de proteção de dados pessoais.

Segundo objetivo específico é a abordagem da LGPD em si, na qual se analisa seus aspectos gerais, os fundamentos, princípios, direitos dos titulares de dados, as bases legais taxativas para tratamento de dados pessoais, as diretrizes de segurança e boas práticas, e, por fim, a ANPD (Autoridade Nacional de Proteção de Dados).

Como terceiro objetivo específico, já atinente às nuances afeitas ao *data protection officer*, examina-se a sua origem e atual situação na GDPR e na LGPD, suas funções, a possibilidade de ser o DPO uma pessoa natural ou jurídica, suas qualificações e a sua publicização, o possível conflito de interesses no exercício das funções de DPO somado ao exercício de outras funções, inclusive, no que tange à pessoa do advogado, a obrigatoriedade do DPO, também do ponto de vista das diferentes formatações empresariais e, também, a possibilidade de compartilhamento do DPO externo, a autonomia e a documentação dos atos do encarregado, e, por fim, se examina o tema da responsabilidade civil e penal.

2 CONTEXTO DA LGPD

Compreender a figura do DPO na LGPD demanda análise das premissas contextuais histórico-econômicas e jurídicas em que a LGPD se insere.

Para tanto, se torna relevante o entendimento sobre a atual economia da informação, o direito à privacidade e o seu consectário direito à proteção dos dados pessoais em um contexto histórico global, mormente para fins da análise comparada com a GDPR que integra a figura do DPO em seu emaranhado legislativo de proteção de dados pessoais.

2.1 A economia da informação

Nesse sentido, na ciência jurídica e fora dela, o debate sobre a proteção de dados pessoais decorre do atual contexto da economia da informação.

Antes de se abordar, especificamente, o tema da economia da informação, como premissa, aborda-se, conforme os escopos deste trabalho, o conceito de "informação".

A despeito de não se objetivar aqui encerrar um conceito de informação, até porque a própria literatura especializada afirma a grande dificuldade de fazê-lo, é notável o esforço de Buckland (1991) para avançar, de alguma forma, nesse caminho espinhoso, de modo que referido autor trabalha com os conceitos de "informação-como-processo", "informação-como-conhecimento" e "informação-como-coisa".

A informação-como-processo, ocorre quando se modifica aquilo que é sabido por uma pessoa diante da comunicação de um fato, ganhando o termo "informação", sob essa ótica, o sentido de "o ato de informar" (BUCKLAND, 1991).

Por sua vez, a informação-como-conhecimento é utilizada para denotar o que é apreendido na "informação-como-processo", ou seja, o conhecimento que é transmitido, relativo a algum fato, assunto ou evento. Nesse sentido, a informação-como-conhecimento é intangível, diante do grau de subjetividade envolvido, visto que depende de convicções pessoais, de maneira que não pode ser medida (BUCKLAND, 1991).

A informação-como-coisa ocorre quando o termo "informação" se relaciona a objetos, quer dizer, quando a informação está registrada. Por essa razão, ela é classificada como tangível (BUCKLAND, 1991).

O próprio autor, afirma, no início de seu texto, a dificuldade de se conceituar "informação", e deixa claro que as definições que apresenta podem não ser

satisfatórias, podem ser confusas, de modo que procura, entretanto, identificar os principais usos da palavra, para que possa haver, ao menos, algum progresso acerca de tal definição (BUCKLAND, 1991).

Diante do objetivo geral deste trabalho, é oportuno consignar que Buckland (1991) menciona que “dados” advém da palavra “datum”, em latim, cujo significado se resume a “coisas que podem ser dadas”. O autor argumenta que referido termo constituir um “termo aceitável para o significado de informação-como-coisa que tenha sido processada de alguma forma para uso posterior” (BUCKLAND, 1991).

De outro lado, Doneda (2019, p. 136) explica que os termos “informação” e “dados” muitas vezes acabam se transpondo, de modo a se poder admitir certa promiscuidade em assim utilizá-los. Todavia, busca distingui-los, distinção esta em que se pode observar encontro com as percepções de Buckland:

> [...] o dado apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de “pré-informação”, anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza (DONEDA, 2019, p. 136).

Pode-se observar, assim, que a definição de Doneda sobre informação, de certa forma, se adequa ao conceito de Buckland quando este se refere à “informação-como-processo”, na medida em que Doneda ressalta a redução do estado de incerteza, e, ainda, quando expõe que a representação contida no dado chega ao limiar da cognição, há correspondência com o conceito de informação-como-conhecimento de Buckland.

O dado, por sua vez, se alocaria em um estado anterior à informação, como afirmado, de maneira que a informação se extrairia por meio do processo interpretativo dos dados.

De forma a trazer-se a discussão sobre informação, dado e dado pessoal, pode-se depreender, pelo delineado, que a informação, no sentido de informação-como-processo apontada por Buckland, configura elementos que têm o potencial de redução do estado de incerteza, ao passo que o dado se encerra em elementos que pressupõem essa redução de estado de incerteza porque precisam ser interpretados,

associados, para que então, após esse processo de cognição, constituam efetivamente uma informação.

Desse modo, o dado pessoal pode ser concebido como aqueles elementos que, interpretados, passados pelo limiar da cognição, se caracterizariam como informações relacionadas a uma pessoa, ou seja, promovendo-se a redução do estado de incerteza relacionado a uma pessoa natural, identificada ou identificável como preconiza o Art. 5º, inciso I, da LGPD (BRASIL, 2018).

Dessa forma, entendidos os possíveis conceitos de informação e a relação da informação com os dados e os dados pessoais, passa-se à análise acerca do tema economia da informação.

A economia da informação se insere, antes, na sociedade da informação. Para Gouveia (2004):

> A Sociedade da informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação.

A sociedade da informação, assim, baseia-se em tecnologias da informação e comunicação, bases estas que se inserem nos contextos sociais de forma a expandir a comunidade local e global. Essa ruptura, apontada por Gouveia, possui para Castells (2000) as seguintes características: o ser humano atua sobre a informação propriamente, fazendo dela a sua matéria prima; as novas tecnologias têm grande potencial de adesão, devido ao fato de a informação ser intrínseca à atividade humana; a lógica de redes passa a predominar devido às novas tecnologias; a tecnologia flexibiliza os processos; a interligação crescente das tecnologias em diferentes áreas do conhecimento.

No início da década de 1990, Fernandes (1991) escreveu o artigo “Economia da informação”, analisando o tema da economia da informação sob a luz dos conceitos de custos, eficácia, eficiência e valor dentro da teoria econômica.

Como resultado de seu trabalho científico, concluiu que “[...] o primeiro passo já foi dado com a crescente conscientização dos especialistas da área da necessidade

de visualizar a informação como um bem econômico e, a partir daí, trata-la como tal" (FERNANDES, 1991, p. 168).

Braman (2005, p. 12) explica que não foi tudo que os economistas consideraram como um bem de valor econômico, tendo em vista que no século XVIII veio à tona o conceito segundo o qual têm valor econômico os chamados "fatores de produção", que haviam sido identificados como terra, trabalho e capital, de maneira que informação, conhecimento, outras ferramentas ou tecnologias não foram inicialmente classificados como bens de valor econômico.

E não que tal conceito não fosse alvo de críticas, conforme argumentou Boulding (1984, p. viii): "O que poderia ser chamado de um livro de receitas da teoria da produção – vindo a produção da mistura da terra, trabalho e capital, e daí saem batatas e automóveis – é uma simplificação exagerada e absurda"[1].

Citado autor, portanto, se irresigna contra o conceito que encerra o bem de valor econômico como aquele que agrega terra, trabalho e capital. Em seguida, inclusive, equipara a definição dos fatores de produção à tentativa medieval dos alquimistas no sentido de transformarem os elementos: "Os fatores de produção são quase tão inúteis quanto as tentativas dos alquimistas de transmutar elementos. A produção [...] sempre começa com o *know-how*"[2] (BOULDING, 1984, p. viii, apud BRAMAN, 2005, p. 13).

Vinte e três anos depois das considerações de Fernandes e trinta após as críticas de Boulding, em 2014 a *Facebook Inc.* adquiriu por US$ 22 bilhões o aplicativo de mensagens *WhatsApp* que havia tido um prejuízo de US$ 130 milhões no ano anterior. O valor do *WhatsApp*? Dados. Por dia, são enviadas 55 bilhões de mensagens por meio do aplicativo que é eminentemente gratuito (BARIFOUSE, 2018).

O *WhatsApp* que, de início, por meio de seus fundadores, garantiu que não iria operar a venda de dados, passou a fazê-lo um ano e meio depois de ter sido adquirido pela *Facebook Inc.*, atualizando seus termos de uso para permiti-lo (BARIFOUSE, 2018).

---

[1] What might be called a cookbook theory of production – that production comes from mixing together land, labor, and capital and out comes potatoes or automobiles – is a preposterous oversimplification.
[2] Production functions are almost as worthless as the alchemists' attempts to transmute elements. Production […] always begins with know-how.

A mudança da política de privacidade para explorar a venda de informações explica a aquisição bilionária da empresa que, contabilmente, tem resultados negativos por oferecer o serviço gratuitamente. Em janeiro de 2019, o *WhatsApp* se tornou o aplicativo mais popular do mundo, com 1,5 bilhões de usuários (ALVES, 2019).

Dessa forma, se em 1991 Fernandes concluía que se estava dando um passo para entender a informação como um bem de valor econômico, nos últimos anos "dados são o novo petróleo", afirmação que constitui um verdadeiro mantra sempre "repetido por consultores, executivos e interessados na digitalização" (RENNAN, 2019). "A diferença é que o petróleo vai acabar um dia. Os dados, não", afirmou Ajay Banga, CEO (*Chief executive officer*) global da Mastercard (RENNAN, 2019).

Outrossim, segundo Shapiro e Varian (1999, p. 3) "tudo o que puder ser digitalizado – codificado sob um fluxo de bits – é informação"[3]. Ainda, para citados autores, a informação possui diferentes valores para cada público consumidor, como entretenimento ou informações financeiras, entretanto, de qualquer modo, as pessoas estão dispostas a pagar pela informação e valorizam específicos bens de informação (SHAPIRO; VARIAN, 1999, p. 3).

Nesse sentido, a economia da informação pode ser definida pela composição de "atividades heterogêneas, incluindo a fabricação de equipamentos eletrônicos, de informática e de telecomunicações e a prestação de serviços de informação: telecomunicações, software, serviços de TI e de conteúdo e mídia" (PORCARO; JORGE, 2013, p. 39).

Diante desse cenário, é incontestável a relevância econômico-social da informação, daí porque é consequência a sua relevância jurídica. A economia da informação é, pois, fato, ao que se agrega valor e, por consequência, resulta a normatização jurídica, neste caso, no Brasil, e neste estudo, a LGPD, porquanto "o mundo jurídico é formado de contínuas 'intenções de valor' que incidem sobre uma 'base de fato', refragendo-se em várias proposições ou direções normativas, uma das quais se converte em norma jurídica em virtude da interferência do Poder" (REALE, 1994, p. 124).

[3]anything that can be digitized – encoded as a stream of bits – is information.

Nesse contexto da economia da informação, duas mudanças, uma de quantidade e uma de qualidade, explicam o novo padrão econômico em relação ao processamento de informações.

Antes desse novo paradigma, a informação era entregue somente por meio de átomos: jornais, revistas e livros físicos. No atual cenário, porém, é entregue por meio de bits. “Um bit não tem cor, tamanho ou peso, e pode viajar na velocidade da luz. É o menor elemento atômico no DNA da informação”[4] (NEGROPONTE, 1995).

Dos átomos aos bits, portanto, é a mudança verificada na nova vida digital, como perpetuou Negroponte (1995) em *Being digital*. O cotidiano é repleto de exemplos da conversão dos átomos, da matéria, para os bits. Em um *smartphone*, por exemplo, podemos utilizar incontáveis aplicações que substituíam bens de valor antes ofertados em matéria: calendário, agenda, calculadora, bloco de notas, despertador, jogos, mensageiros. Na área jurídica, como outro exemplo, hoje se observa a quase completa digitalização de todos os novos procedimentos processuais no Poder Judiciário Nacional, em substituição aos robustos volumes de autos que ganhavam destaque nas prateleiras dos fóruns, nos escritórios de advocacia, de defensores e procuradores.

Com base nas lições do citado autor, Bioni (2019, p. 36), explica que se antes a coleta, transferência, armazenamento, etc., de informações era feita em papel, passou a ser feita em bits, por meio do sistema binário de dígitos, facilitando o acúmulo de uma quantidade de informação muito maior do que seria possível acumular em papel. É a mudança quantitativa.

É característica, portanto, dessa economia da informação, converter-se todo e qualquer tipo de conhecimento e informação para meios eletrônicos, reduzindo-se cada vez mais a matéria (LASTRES; FERRAZ, 1999, p. 47).

De outro lado, ainda, encontrar uma informação em um meio físico depende, em primeiro lugar, da organização do arquivo. E mesmo que esteja organizado esse arquivo, será necessário vasculha-lo para encontrar a informação desejada. Já no meio digital, basta utilizar o campo de busca e indexar as palavras-chave que a informação será facilmente encontrada por meio do nome do documento ou mesmo pelo próprio conteúdo do documento, o que potencializa a possibilidade de localização (BIONI, 2019, p. 36). É a mudança qualitativa.

---

[4]A bit has no color, size, or weight, and it can travel at the speed of light. It is the smallest atomic element in the DNA of information.

E a essas referidas mudanças quantitativas e qualitativas, soma-se ainda o fator internet, que, assim, em conjunto, implicaram a virtualização da informação (BIONI, 2019, p. 36) e o “novo padrão tecno-econômico baseado nas tecnologias de informação e outras das então denominadas tecnologias avançadas (biotecnologia, materiais avançados, química fina e mecânica de precisão)” (LASTRES; FERRAZ, 1999, p. 38), o que resultou o rompimento da dinâmica tecnológica internacional, antes baseada em tecnologias de matéria e energia, para uma nova dinâmica baseada em informação, flexíveis e computadorizadas (MALDONADO, p. 105).

Nesse sentido, cumpre citar que Giddens (1991, p. 111-113) trata de risco e perigo como um aspecto ameaçador no mundo moderno. Assim, classifica esse perfil de risco em sete itens, os quais se subdividem em dois grandes grupos, quais sejam, o primeiro grupo, relativo à distribuição objetiva dos riscos e o segundo, referente à vivência do risco ou à percepção dos riscos percebidos.

De tais riscos, o primeiro se refere à intensidade do risco, de modo que a intensidade se caracteriza como o elemento básico do aspecto ameaçador, podendo-se notar a guerra nuclear como um exemplo, tendo em vista que se trata de um risco globalizado, em que se quebra a barreira “dos outros”. Referido autor utiliza a guerra nuclear como exemplo de globalização do risco no sentido de intensidade devido a sua capacidade de ameaça à sobrevivência da humanidade (GIDDENS, 1991, p. 111-113).

Quando se menciona a quebra da barreira “dos outros”, indica-se que o risco é irrestrito, independentemente de classes sociais ou quaisquer outras barreiras que dividam ou classifiquem os seres humanos, tendo em vista que tais riscos se põem com potencial à completa destruição do planeta Terra: “Esta circunstância justifica inteiramente a afirmação de que em tal contexto, não existem mais ‘outros’: tanto os combatentes quanto os que não estão envolvidos, sofrerão” (GIDDENS, 1991, p. 113).

Vai ao encontro do risco no aspecto da intensidade, elencado por Giddens, o que se compreende, hoje, na economia da informação, pelos chamados “filtros-bolha”.

Os filtros-bolha têm origem no objetivo de tornar a navegação do usuário mais agradável, mais otimizada e personalizada, de modo que, ao fazer uso de aplicações, pudesse com mais facilidade, encontrar os conteúdos de sua preferência (MAGRANI, 2014, p. 118). Nesse sentido, a “[...] Filter Bubble (ou filtros-bolha), pode ser definida como um conjunto de dados gerado por todos os mecanismos algorítmicos utilizados

para se fazer uma edição invisível voltada à customização da navegação *on-line*" (MAGRANI, 2014, p. 118).

Foi necessária a criação dos filtros-bolha devido à sobrecarga de informações, o que implica duas consequências: a primeira, a filtragem não intencional (do ponto de vista do usuário, mas intencional do ponto de vista do provedor de aplicação), que é o próprio filtro-bolha; e segunda, a filtragem voluntária feita pelos próprios usuários, já após a filtragem não intencional, que acaba por reforçar, reafirmar, o filtro-bolha (MAGRANI, 2014, p. 119).

A forma como os filtros agem atualmente mostra o que entende ser do interesse do usuário, mas oculta aquilo que o usuário deseja ou precisa ver, de maneira a restringir direitos e garantias fundamentais, a autonomia dos indivíduos, a liberdade de expressão, a comprometer, portanto, a reflexão, o debate e as escolhas dos usuários (MAGRANI, 2014, p. 119).

> O professor de *Harvard*, *Lawrence Lessig*, chamou a atenção para o fato de que a própria arquitetura da internet, ou seja, dos *hardwares* e *softwares* que a acompanham, com estruturação técnica e códigos que regem seu funcionamento, são também formas de regular o comportamento humano. Formas essas por vezes tão eficientes quanto outras formas mais conhecidas como o Direito, a economia, e as normas sociais. Por isso, cunhou a conhecida frase "*code is law*", uma vez que a própria arquitetura dos sites nos deixa reféns dos algoritmos, regulando nosso comportamento, assim como o Direito, e criando obstáculos sérios ao acesso à informação, à autonomia individual, à privacidade e à liberdade de expressão (MAGRANI, 2014, p. 120).

Pode-se assim, notar que os filtros-bolha vão ao encontro do risco no aspecto da intensidade, conforme enunciado por Giddens, muito antes, em 1991, tendo em vista o potencial comprometedor de diversos direitos e garantias fundamentais de todos os indivíduos, de forma irrestrita, sem limitações a classes, limitações territoriais, ou quaisquer outras, estando exposto, portanto, aos riscos comprometedores do filtro-bolha, simplesmente por serem usuários de quaisquer aplicações que utilizem tal arquitetura.

Isso exposto, relevante demonstrar o atual estágio do uso de tecnologias da informação no Brasil, a trazer, portanto, referido debate para dentro do contexto brasileiro, mormente quanto ao crescente número de usuários das tecnologias da informação.

Na última pesquisa, publicada em 2018, sobre uso das tecnologias da informação e comunicação nas empresas brasileiras, publicada pelo Comitê Gestor

da Internet no Brasil, se verifica que em 2017 “[o] uso de computadores e Internet entre as empresas brasileiras se encontra amplamente disseminado – a maioria delas usa computadores (98%) e possui acesso à Internet (98%) – independentemente da estratificação selecionada” (COMITÊ..., 2018, p. 118), o que demonstra a quase integral aderência das empresas brasileiras às tecnologias da informação.

Além disso, relevante dado da pesquisa demonstra que “[s]eja por porte, por região geográfica ou por atividade econômica, mais de 90% das empresas possuem computador e acesso à Internet” (COMITÊ..., 2018, p. 118), dados também de 2017.

Já na pesquisa sobre uso das tecnologias de informação e comunicação nos domicílios brasileiros, publicada em 2019 também pelo Comitê Gestor da Internet no Brasil, se constatou que “[e]m 2018, o acesso à Internet estava presente em cerca de 46,5 milhões de domicílios brasileiros, número que equivale a 67% deles, seis pontos percentuais a mais do que em 2017 (61%)” (COMITÊ..., 2019, p. 103), número que fica ainda mais expressivo se comparado com os dados de 2008 que demonstravam que apenas 18% dos domicílios brasileiros tinham acesso à internet (COMITÊ..., 2019, p. 104).

Além disso, “A proporção de usuários de Internet no Brasil, embora estável em relação a 2017 (67%), continuou seguindo a tendência de crescimento observada nos últimos anos, chegando a 70% em 2018” (COMITÊ... 2019, p. 103). Referido dado “representa uma estimativa de 126,9 milhões de indivíduos com dez anos ou mais conectados à rede” (COMITÊ... 2019, p. 103), sendo que dentre os usuários da internet, “quase a totalidade utilizou a rede pelo telefone celular (97%), e a maior parte (56%) usou a rede exclusivamente por esse dispositivo” (COMITÊ... 2019, p. 103).

Quanto ao comércio eletrônico, 34% dos usuários de internet realizou uma compra de produtos ou serviços nos últimos 12 meses anteriores à pesquisa, comparado com 31% no ano de 2012, o que representa um crescimento de 19 milhões de usuários (COMITÊ... 2019, p. 103).

Desse modo, verifica-se a ruptura do padrão econômico, passando-se de uma economia materializada, baseada em átomos, a uma economia baseada em bits, centrada nas tecnologias da informação, em que a informação se evidencia como bem de valor econômico, e se passa a ter um enorme potencial de acúmulo de informação, somado ao elevado potencial de busca dessa informação.

Verifica-se, ainda, no Brasil, um contexto da difusão, em expansão, das tecnologias da informação, que abrange quase 100% das empresas do território

nacional, chegando-se a um percentual de expressivos 90% das empresas, independentemente do porte, da região ou do tipo de atividade econômica desenvolvida.

Quase 100% das empresas brasileiras, portanto, detém dispositivos computacionais e acesso à internet, encontrando-se, assim, no contexto de virtualização da informação, de modo que passam a beneficiar-se das mudanças quantitativas e qualitativas para o tratamento das informações.

E se não bastasse isso, a despeito do potencial de coleta de informações por todas as quase 100% empresas brasileiras ainda que por meios físicos, considere-se que 67% dos brasileiros com mais de dez anos tem acesso à internet, potencializando, – em virtude da velocidade que os bits trazem, conforme assinalou Negroponte – o acúmulo e o tratamento dessas informações por parte desses agentes econômicos.

O cenário brasileiro, assim, é apenas um exemplar da economia da informação, refletindo a alteração do paradigma econômico mundial.

É neste contexto que se inserem os massificados questionamentos sobre o tratamento dessas informações e, em especial a esta pesquisa, sobre o tratamento dos dados pessoais, que passam a ser debatidos diante do valor econômico que os dados detêm nessa nova economia, em confronto com o direito à privacidade e à proteção de dados pessoais dos sujeitos inseridos nesta nova economia.

2.2 O direito à privacidade

Nesta seção, aborda-se o direito à privacidade em duas frentes: primeiro, se projeta uma retrospectiva histórica de importantes documentos que o citam; segundo, se realiza a análise da previsão constitucional da intimidade e da vida privada, de maneira a se abordar as respectivas definições e indefinições.

Dessa maneira, é possível encontrar menções do direito à privacidade em diversas civilizações antigas, como na chinesa, na hebraica e grega, além de haver diversas menções e raízes do referido direito na idade média e na idade moderna, a haver, ainda, disposições embrionárias da proteção à privacidade na Europa mormente à época do liberalismo clássico, berço do liberamos jurídico.

Entretanto, para o propósito deste trabalho, tendo em vista o objetivo geral de analisar a figura do DPO, e não de enveredar a busca histórica completa de indícios do direito à privacidade na história, recorta-se a análise deste tema para a partir dos anos finais do século XIX, em que se iniciaram os debates sobre a privacidade no

contexto das tecnologias da época, como fotografia e mídia impressa, e se iniciou o delineamento das primeiras faces que tomou o direito à privacidade como um direito institucionalizado nos atuais ordenamentos jurídicos mundo afora.

Uma detalhada e crítica retrospectiva histórica do direito à privacidade, todavia, pode ser depreendida da importante obra de Doneda (2019) sobre o tema da privacidade e da proteção dos dados pessoais, à qual se remete o leitor para aprofundamento histórico – obra da qual, inclusive, se vale esse trabalho no que pertine ao recorte metodológico realizado.

Pois bem.

Em seus primeiros contornos, surge o direito à privacidade como um direito negativo, com o intuito de proteger o indivíduo das ingerências de terceiros em sua esfera privada, longe da perspectiva que se visualiza atualmente em sistemas jurídicos que visam a proteção de dados pessoais, nos quais os textos normativos impõem a adoção de posturas positivas quanto ao tratamento de dados pessoais.

Não se pode deixar de mencionar em qualquer estudo sobre o direito à privacidade, o célebre artigo publicado por Warren e Brandeis (1890), intitulado “O direito à privacidade” *The right to privacy*, estudo este que marca a institucionalização do direito à privacidade como hoje é reconhecido.

Em referido artigo, os autores, então advogados em Boston, buscam analisar se o direito dos Estados Unidos da América disporia de algum princípio que pudesse ser invocado a fim de proteger a privacidade dos indivíduos e, se existe, qual a natureza e extensão de tal proteção: “[o] propósito é verificar se a lei vigente admite um princípio a ser invocado para proteger a privacidade do indivíduo e, caso o faça, verificar qual a natureza e extensão dessa proteção”[5] (WARREN; BRANDEIS, 1890, p. 197).

Os autores iniciam o texto contextualizando a proteção que a lei sempre ofertou para violações físicas à vida e à propriedade, a enfatizarem que o direito à vida sempre visou proteger o indivíduo de violações físicas, de forma que a liberdade sempre significou liberdade de restrições reais, físicas, e o direito à propriedade garantiu as terras e castelos dos indivíduos (WARREN; BRANDEIS, 1890, p. 193).

Assim, a lei sempre projetou a proteção à vida e à propriedade em suas dimensões físicas, palpáveis, sendo esses os substratos de toda a proteção jurídica.

---

[5]It is our purpose to consider wheter the existing law afford a principle which can properly be invoked to protect the privacy of the individual; and if it does, what the nature and extent of such protection is.

Entretanto, explicam, tais direitos passaram a ter uma abrangência maior, de forma que o direito à vida superou a esfera física: "[...] e agora o direito à vida passou a significar o direito de aproveitar a vida, o direito de ser deixado em paz; o direito à liberdade assegura o exercício de amplas liberdades civis"[6] (WARREN; BRANDEIS, 1890, p. 193).

No mesmo passo, o direito à propriedade, no decorrer da história, deixa de abarcar apenas as propriedades materiais: "[...] e o termo 'propriedade' evoluiu para abranger todas as formas de posse – tangíveis e intangíveis"[7] (WARREN; BRANDEIS, 1890, p. 193).

Portanto, as violações originariamente rechaçadas pela lei sempre foram violações físicas, fossem tais agressões contra a vida ou contra a propriedade, de maneira que tão somente com a evolução das instituições jurídicas é que a lei passou a reconhecer a antijuridicidade de violações aos aspectos imateriais da vida e da propriedade.

Nesse sentido, argumentam que como extensão do direito à vida, para a proteção contra barulhos, odores, poeira e fumaça, surgiu a lei do incômodo. Daí que as emoções humanas passaram a ser protegidas além do corpo do indivíduo, passando-se a proteger dimensões não corpóreas, como a reputação, como quando surgiu a lei da calúnia e difamação (WARREN; BRANDEIS, 1890, p. 194).

E acompanhando a tendência, o direito à propriedade se expande para um direito incorpóreo, "[...] e depois, se abiu o vasto campo da propriedade imaterial, nos produtos e processos da mente, como obras literárias, *goodwill*, segredos comerciais e marcas"[8] (WARREN; BRANDEIS, 1890, p. 194-195).

> Esse desenvolvimento do direito era inevitável. A intensa atividade da vida intelectual e emocional e o ápice das sensações que vieram com o avanço do processo civilizatório, deixaram claro ao homem que somente parte da dor, do prazer e dos benefícios está nas coisas físicas. Pensamentos, emoções e sensações exigiam reconhecimento jurídico, e a bela capacidade de evolução que caracteriza a *common law* possibilitou que os juízes conferissem a proteção necessária, sem intervenção legislativa[9] (WARREN; BRANDEIS, 1890, p. 195).

---

[6] […] and now the right to life has come to mean the right to enjoy life, - the right to be let alone; the right to liberty secures the exercise of extensive civil privileges.

[7] […] and the term "property" has grown to comprise every form of possession – intangible, as well as tangible.

[8] […] and then there opened the wide realm of intangible property, in the products and processes of the mind, as Works of literature and art, goodwill, trade secrets, and trade marks.

[9] This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations

O contexto histórico em que se insere a discussão relativa à privacidade levantada por Warren e Brandeis é muito bem exposto no texto e está atrelado sobretudo à fotografia e à imprensa e explicam por que esse primeiro contorno do que hoje é concebido como direito à privacidade, foi assim delineado como um direito de não ser incomodado, de ser deixado a sós, de não ter a casa e a vida doméstica publicizadas sem prévia autorização do indivíduo.

Para os autores, assim, a fotografia e a imprensa jornalística invadiram a vida privada e doméstica, e são tratados como um verdadeiro mal que atingia a sociedade, caracterizando-se a imprensa como uma violadora dos limites da propriedade e da decência, que transforma a fofoca em um produto para alimentar desocupados (WARREN; BRANDEIS, 1890, p. 195-196).

Os autores chamam atenção à capacidade de circulação de fofocas por meio da imprensa, consignando que por mais inofensiva que seja, quando amplamente e persistentemente divulgada, tem potencial de diminuir o indivíduo (WARREN; BRANDEIS, 1890, p. 196).

É esse o contexto em que se insere o célebre artigo, amplamente citado em qualquer estudo sobre privacidade. Como anteriormente mencionado, o propósito da pesquisa de Warren e Brandeis era desvendar na ordem jurídica estadunidense algum princípio que amparasse a proteção à privacidade.

Os autores, assim, fazem uma análise doutrinária a fim de evidenciar o direito à privacidade (WARREN; BRANDEIS, 1890, p. 198-212), analisando precedentes sobre direito à propriedade, direitos autorais, difamação, confiança e violações contratuais.

Com base na análise de tais casos, os autores concluíram que o que está por trás das garantias encontradas não é apenas o direito à propriedade (a não ser que se estendesse tal conceito), mas sim o direito à privacidade:

> O princípio que garante proteção aos escritos pessoais e a quaisquer outras produções intelectuais ou emocionais é o direito à privacidade, e o direito não tem nenhum novo princípio a elaborar quando estende essa proteção à aparência da pessoa, os seus dizeres, condutas e suas relações pessoais domésticas ou quaisquer outras[10] (WARREN; BRANDEIS, 1890, p. 213).

demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.

[10] The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.

Após referida conclusão, Warren e Brandeis (1890, p. 214 a 218) realizam seis delimitações ao direito à privacidade: 1. Publicações de interesse público ou de interesse geral não estão protegidas pelo direito à privacidade; 2. Publicações, de qualquer que seja a natureza privada, não estão proibidas se houver autorização legal pela lei de calúnia e difamação; 3. Publicações orais sem possibilidade de danos efetivos não violam a privacidade; 4. Se houver publicação de fatos pelo próprio indivíduo ou se houver seu consentimento, não há proteção do direito à privacidade; 5. Haverá violação à privacidade mesmo que o conteúdo publicado seja verdadeiro; 6. Haverá violação à privacidade ainda que não haja malícia por parte daquele que publica o conteúdo. E por fim, apresentam instrumentos para os casos de violação à privacidade (WARREN; BRANDEIS, 1890, p. 219-220).

Como visto, Warren e Brandeis definiram os primeiros contornos do direito à privacidade como um direito institucionalizado, extraindo-o de diversos precedentes, e, assim, determinando os seus limites de aplicação.

Importante consignar que não foram Warren e Brandeis que cunharam o termo “direito de ser deixado em paz”[11]. Como os próprios autores mencionam, tal termo foi atribuído ao conteúdo do que hoje se entende por direito à privacidade pelo Juiz Cooley: “Recentes invenções e modelos de negócios chamam atenção quanto ao próximo passo a ser dado para proteção da pessoa a fim de garantir ao indivíduo o que o Juiz Cooley chama de ‘direito de ser deixado em paz’”[12] (WARREN; BRANDEIS, p. 195).

Portanto, poucos antes anos, Cooley (1888, p. 29), definindo conceitos legais, tratou do direito de ser deixado em paz: “Pode-se dizer que o direito da pessoa é um direito de total imunidade: o direito de ser deixado em paz”[13].

Por isso, seria equivocado entender o artigo de Warren e Brandeis como uma referência isolada, pois se insere em um contexto de encontro dos Estados Unidos com a economia capitalista, e o debate sobre privacidade já se tinha feito presente na jurisprudência americana, como no caso *Pope v. Curl*, de 1741, o qual tratou da correspondência entre o poeta Alexander Pope e o romancista Jonathan Swift, citado

[11] Right to be let alone.
[12] Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone”.
[13]The right to one's person may be said to be a right of complete immunity: to be let alone.

como a mais antiga discussão na *common law* sobre privacidade (DONEDA, 2019, p. 124-125).

Doneda (2019, p. 126-127) menciona que mais que uma preocupação acadêmica de definir o conceito de privacidade, trata-se de uma necessidade real no contexto do fluxo de informações e cita que hoje a preocupação ultrapassa notícias sobre festas privadas e alcançam situações como o tratamento de informações por empresas estrangeiras: “como as informações que uma empresa de assistência médica mantém, em Hong Kong, sobre nossas informações genéticas e hábitos alimentares, por exemplo”.

E é relevante aqui consignar, que foi concebido o direito à privacidade em uma perspectiva negativa, de não violação, de não intromissão na esfera privada.

Em abril 1948, a Declaração Americana dos Direitos do Homem, aprovada em Bogotá na IX Conferência Internacional Americana, foi o primeiro instrumento de publicidade internacional[14] a prever o direito à privacidade, em seu Art. (artigo) 5º: “Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular” (DECLARAÇÃO..., 1948).

Nota-se que o direito à privacidade segue a linha orientada por Warren e Brandeis, como um direito de não ser incomodado, de o indivíduo ter a sua esfera privada, sua vida privada e domiciliar, não expostos.

Meses após, a Declaração Universal dos Direitos Humanos, em dezembro de 1948, previu também o direito à privacidade em seu Art. 12: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (ASSEMBLEIA..., 1948).

Novamente, se depreende o direito à privacidade como uma proteção do indivíduo contra ingerências externas em sua esfera particular.

No mesmo sentido, após dois anos, em 1950, na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais”, provada em Roma, previu em seu Art. 1º: “Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência” (CONSELHO..., 1950).

[14] Discute-se a validade jurídica da Declaração Americana dos Direitos do Homem, tendo em vista que não foi incluída na Carta da OEA, criada na mesma data, e porque não foi ratificada por Estados signatários para se caracterizar como um tratado internacional. Por essa razão, a referida Declaração é mencionada aqui como o primeiro instrumento de publicidade internacional a prever o direito à privacidade, sem mencioná-lo como um tratado internacional.

Em 1966, o Pacto Internacional sobre Direitos Civis e Políticos, aprovado na Assembleia Geral das Nações Unidas, também ratificou a proteção à vida privada:

> 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honras e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas. (ASSEMBLEIA..., 1966).

Não muito após, a conferência nórdica sobre direito à privacidade, em 1967, em Estocolmo, foi a primeira conferência internacional a tratar exclusivamente sobre o direito à privacidade e estabeleceu diversas diretrizes que servem até hoje como linhas gerais para compreensão de tal direito.

Na parte I das conclusões, a convenção prevê que o direito à privacidade é de suma importância para a felicidade humana e que deve ser reconhecido como um direito humano. Na mesma esteira do que consignaram o Juiz Cooley e Warren e Brandeis, a convenção expressa que "[o] direito à privacidade é o direito de ser deixado a sós para que se possa viver sua própria vida com o mínimo grau de interferência"[15].

Ainda nas conclusões da conferência nórdica de 1967, listou-se situações práticas que buscavam ser abrangidas pela definição do direito à privacidade, e, assim, o item 3 da convenção cita doze situações exemplares:

> (i) localização da pessoa;
> (ii) entrada e busca nas instalações ou outros bens;
> (iii) exames médicos, psicológicos e físicos;
> (iv) declarações infundadas ou irrelevantes e vexatórias sobre uma pessoa;
> (v) interceptação de correspondência;
> (vi) escutas telefônicas ou por fio;
> (vii) uso de vigilância eletrônica ou outros dispositivos de "escuta";
> (viii) gravação, fotografia ou filmagem;
> (ix) importunação pela imprensa ou por agentes de outros meios de comunicação social;
> (x) divulgação pública de fatos privados;
> (xi) divulgação de informação dada ou recebida de profissionais ou a autoridades públicas obrigadas a guardarem sigilo;
> (xii) assediar uma pessoa (por exemplo, observá-la e importuná-la ou submetê-la a ligações telefônicas incômodas). (CONFERÊNCIA..., 1967).[16]

---

[15] The Right to Privacy is the right to be let alone to live one's own life with the minimum degree of interference.

[16] (i) search of the person; (ii) entry on and search of premises or other property; (iii) medical examinations, psychological and physical tests; (iv) untrue or irrelevant embarrassing statements about a person; (v) interception of correspondence; (vi) wire or telephone tapping; (vii) use of electronic surveillance or other " bugging " devices; (viii) recording, photographing or filming; (ix) importuning by the press or by agents of other mass media; (x) public disclosure of private facts; (xi) disclosure of

A conferência nórdica de 1967, portanto, concretiza o que se verificou nos documentos internacionais citados quanto à definição do direito à privacidade: ser deixado em paz, sem interferências, sem intromissões, ou, com a menor intromissão possível na esfera privada do indivíduo.

É possível, dessa forma, observar que desde o final do século XIX um grande movimento, globalizado, com vistas ao reconhecimento do direito à privacidade, ganhou corpo com a identificação da privacidade em relevantes instrumentos internacionais.

No Brasil, a Carta Magna de 1988, consagrou o direito à privacidade como um direito fundamental, previsto no Art. 5º, inciso X, sob os seguintes dizeres: “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”.

Furlaneto Neto e Garcia (2014, p. 773-775) ensinam que o Pacto Internacional sobre Direitos Civis e Políticos proclamou a denominada primeira dimensão de direitos fundamentais, de modo que a previsão constitucional do Art. 5º, X, consagrou, portanto, o direito à intimidade como um direito humano fundamental de primeira dimensão.

Pesaram e pesam até hoje as discussões relativas à diferença entre “intimidade” e “vida privada” dispostas lado a lado no texto constitucional: têm o mesmo sentido? O constituinte pecou pelo excesso? Um termo é mais abrangente que o outro quanto à proteção?

Doneda (2019, p. 98) demonstra ser considerável a abundância de termos que a doutrina brasileira utiliza para definir privacidade, a consignar, ainda, que além de “privacidade” aparecem na literatura jurídica os seguintes termos: “vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como ‘privatividade’ e ‘privaticidade’”.

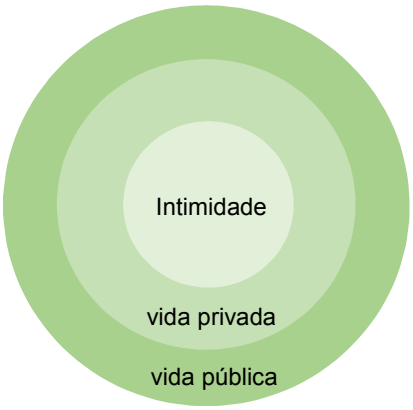
Interessante a menção de Wolff (1991, p. 7), apenas dois anos após a promulgação da CF (Constituição Federal), sobre o imbróglio da definição:

> No Brasil, os autores adotam preferentemente a expressão "Direito à Intimidade", com exceção de René Ariel Dotti, que emprega indistintamente as denominações "direito a vida privada", "direito à

information given to, or received from, professional advisers or to public authorities bound to observe secrecy; (xii) harrassing a person (e.g. watching and besetting him or subjecting him to nuisance calls on the telephone).

> intimidade da vida privada" e "direito à privacidade", e José Afonso da Silva, que acolhe a expressão "direito à privacidade".

Quanto à previsão constitucional, Doneda (2019, p. 103) explica que a definição do constituinte tem raízes na doutrina de Hubmann, que expressa as ideias de intimidade, vida privada e vida pública em um esquema de esferas concêntricas, de modo que dentro do menor entorno se pode observar a intimidade, após, mais abrangente, a vida privada, e, além desta, a vida pública. A doutrina de Hubmann pode ser ilustrada da seguinte forma:



Nota-se, por exemplo, que Moraes (2006, p. 131) segue em certa medida a referida estrutura ao mencionar a interligação entre “intimidade” e “privacidade”, a argumentar, nesse sentido, que a diferença reside na menor amplitude do primeiro termo, inserido no âmbito do segundo, de modo que a “intimidade” envolveria situações mais íntimas, subjetivas, como as relações familiares e de amizade, em aspecto mais privativo do que a “privacidade”, que envolveria outros relacionamentos, objetivos, como relações comerciais, de trabalho e de estudo.

No mesmo sentido, Araújo e Nunes Júnior (2005, p. 139-140) argumentam pela existência de uma divisão da vida social e da vida privada, de modo que dentro da privacidade se inserem os relacionamentos do indivíduo que não estão abertos ao público, como a família, aventuras amorosas, lazer e segredos de negócios, e, assim, dentro deste território privado, sempre que houver espaço para mais de uma pessoa, pode haver a violação de direitos, o que traz importância, portanto, à intimidade. Dessa forma, para explicitar o conteúdo da intimidade, sustentam: “A privacidade resguarda o indivíduo da publicidade. Entretanto, qual seria a proteção jurídica individual em face

de abusos cometidos dentro da esfera privada? Exatamente o direito de intimidade" (ARAÚJO; NUNES JÚNIOR, 2005, p. 140).

Em seguida, Araújo e Nunes Júnior (2005, p. 139-140) expressamente defendem o modelo de compreensão de círculos concêntricos atrás citado: "Poderíamos ilustrar a vida social como um grande círculo, dentro do qual um menor, o da privacidade, em cujo interior seria aposto um ainda mais constrito e impenetrável, o da intimidade".

Miranda (2018, p. 25-26) também anota a doutrina dos círculos concêntricos, de modo que define a privacidade como "o direito de ter respeitada a exclusividade de acesso a determinadas informações, tendo como atributos a solidão (o estar sozinho), o segredo ou sigilo (proteção), e a autonomia da vontade.

Com base em tal definição, explica que no círculo mais abrangente estariam as relações sociais sem proteção ampla, no qual estão inseridas informações mínimas para introduzir o indivíduo na sociedade, como a sua identificação. No círculo intermediário, estariam informações mais restritas, compartilhadas com um número mais exíguo de indivíduos, como família, psicólogos, advogados. E, ainda, no círculo mais apertado, estaria a esfera de segredo ou sigilo, relacionadas a aspectos mais íntimos, como condição sexual, filiação filosófica, política ou religiosa, as quais não detêm absolutamente nenhum interesse público (MIRANDA, 2018, p. 26-27).

Verifica-se, portanto, que a previsão constitucional de um direito à intimidade e um direito à vida privada, separando-os, assim, fez enraizar na literatura jurídica brasileira a diferença no conteúdo entre tais direitos, de modo a viger a compreensão no sentido de que, em geral, existe a vida pública e a vida privada, e, nesta, encontra-se um campo sigiloso, respeitante estritamente aos anseios mais íntimos do indivíduo, atribuindo-se a esse aspecto mais recluso o caráter da intimidade.

Sob esse mesmo prisma, Silva (2006, p. 101), realiza a distinção entre intimidade e privacidade. Para tanto, atribui à intimidade a concepção deflagrada por Dotti (1980, p. 69, apud SILVA, 2006, p. 101): "a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais". Para definir a vida privada, realiza a distinção entre "vida exterior" e "vida interior".

Argumenta, assim, que "[a] *vida exterior*, que envolve a pessoa nas relações sociais e nas atividades públicas, pode ser objeto das pesquisas e das divulgações de terceiros, porque é pública" (SILVA, 2006, p. 101), a qual se contrapõe, portanto, à vida interior "[...] que se debruça sobre a pessoa mesma, sobre os membros de sua

família, sobre seus amigos, é a que integra o conceito de ‘vida privada’" (SILVA, 2006, p. 101).

Como se observa, as perspectivas apresentadas quanto ao direito à privacidade, trazem consigo um conteúdo negativo, em realce à preservação do indivíduo frente a interferências externas. Foi esse o sentido enunciado por Warren e Brandeis, o qual reflete até hoje nos estudos e atividades interpretativas relativas à privacidade.

Tal conteúdo “negativo”, porém, se tornou apenas uma face do direito à privacidade diante da contextualizada economia da informação, a passar a conviver com a outra face, a que exige posturas “ativas” por parte de certos sujeitos a fim de que, dentro dessa esfera privada, seja assegurada a liberdade e os direitos de escolha dos indivíduos.

Conforme acentua Doneda (2018, p. 130), o uso e coleta de informações pessoais implicou uma nova interpretação sobre a privacidade, a qual foi cunhada por Rodotà como “tutela das escolhas de vida contra o controle público e a reprovação social” (RODOTÀ, 1991, p. 202, apud DONEDA, 2018, p. 130). Nesse sentido, Doneda (2018, p. 131-132) apresenta o novo caráter do qual se reveste o direito à privacidade:

> A privacidade assume, então, um caráter relacional, que deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior – pela qual a pessoa determina sua inserção e de exposição; esse processo tem como resultado o fortalecimento de uma esfera privada do indivíduo – esfera que não é a de Hubmann, mas uma que torne possível a construção da individualidade e o livre desenvolvimento da personalidade sem a pressão de mecanismos de controle social.

Segundo a concepção apresentada, portanto, não se limita a privacidade ao direito do indivíduo de se resguardar contra ações externas, mas o de escolher os limites das relações que estabelece com o mundo exterior, para, assim, desenvolver sua personalidade livremente, sem a influência dos mecanismos de controle social.

E é nesse contexto da evolução do conteúdo da privacidade em virtude do massivo tratamento de dados pessoais, e evidentemente, também por causa destes, que se insere a discussão sobre o direito à proteção dos dados pessoais.

Razão de existir do encarregado de proteção de dados (DPO), a LGPD vem a lume em um contexto de evolução internacional sobre a institucionalização de

direitos à proteção de dados pessoais, evoluídos do direito à privacidade, conforme consignado por Doneda.

Desta sorte, na próxima seção se apresenta memória sobre o direito à proteção de dados pessoais, o que provocou a recente aprovação da LGPD no Brasil, na qual se insere a figura do DPO.

2.3 O direito à proteção dos dados pessoais

Realizada a apresentação do direito à privacidade, passa-se, aqui nesta seção, da privacidade à proteção dos dados pessoais, em que se busca: distinguir citados direitos; trazer as primeiras menções históricas sobre proteção de dados pessoais; e, por fim, elencar a evolução legislativa da proteção de dados pessoais sob o contexto global e no Brasil.

Pois bem.

Emaranhados entre si, mas diversos: os direitos à privacidade e à proteção dos dados pessoais têm intrínseca relação, todavia, são diversos, autônomos, inclusive, de forma a imporem cada um com sua força normativa posturas diametralmente opostas aos jurisdicionados.

Rodotà (2008, p. 17) consigna de maneira exemplar a distinção entre o respeito à vida privada e familiar e o direito à proteção dos dados pessoais, a ensinar, assim, que o primeiro visa obstar a interferência na vida privada e familiar da pessoa, impondo, portanto, uma proteção estática, negativa, ao passo que, de maneira oposta, o direito à proteção dos dados pessoais prevê um regramento sobre os mecanismos de tratamento dos dados pessoais: “[...] é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos”.

Conclui, portanto, Rodotà (2008, p. 17), ser a concepção da proteção aos dados pessoais o fim do processo evolutivo do direito à privacidade, a consignar que se passa: “[...] de uma definição original como o direito de ser deixado em paz, até o direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser construída”.

Por sua vez, Bioni (2019, p. 125) sustenta que a distinção entre o direito à privacidade e à proteção dos dados pessoais não pode ser vista meramente como sendo a proteção dos dados pessoais uma evolução, o final da linha, do direito à privacidade, sobretudo porque quando se fala em privacidade, parte-se de uma distinção entre as esferas pública e privada, e quer dizer, assim, que no substrato do

direito à privacidade está distinguir e vedar que se torne público aquilo que é privado: “[n]ão seria a curiosidade do público que romperia as portas impenetráveis do castelo da privacidade”.

O autor explica, portanto, que quando se trata de direito à privacidade: “[o] que é público e privado é o que normatiza o conteúdo do direito à privacidade, sendo a sua lógica centrada na liberdade *negativa* de o indivíduo não sofrer interferência alheia” (BIONI, 2019, p. 125).

E, também com base nas lições de Rodotà, Bioni (2019, p. 126) explica que: “[p]or outro lado, a ‘evolução’ do direito à privacidade, que englobaria o direito à proteção de dados pessoais, consistiria em uma proteção dinâmica e em uma liberdade *positiva* do controle sobre as informações pessoais”.

Entretanto, especifica que o direito à proteção dos dados pessoais, de outro lado, não se limita a esse exercício de distinguir o que diz respeito ao público e o que deve se limitar à esfera privada.

Nesse sentido, “[p]or exemplo, fatos públicos, que a priori não gerariam preocupação atinente à vida privada, podem, quando agregados a outros fatos (dados), revelar detalhes precisos sobre a personalidade de um indivíduo” (BIONI, 2019, p. 126).

Para Bioni (2019, p. 127) “[p]ropugnar que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é uma construção dogmática falha que dificulta a sua compreensão”, e explica, assim, que tal direito foge da distinção entre público e privado na medida em que basta que exista uma informação que se enquadre no conceito de dado pessoal para seja deflagrado referido direito.

Diferentemente do conteúdo do direito à privacidade, cujo substrato se cinge à distinção entre público e privado, quando se trata de proteção de dados pessoais “[...] toda a sua construção é balizada pelo conceito de dado pessoal, o que pode ser vis-à-vis uma informação pública ou privada” (BIONI 2019, p. 126).

Nesse sentido, distintamente do bem jurídico protegido pelo direito à privacidade, o direito à proteção dos dados pessoais “tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade” (BIONI, 2019, p. 127).

Dessa forma, pode-se depreender que o direito à proteção dos dados pessoais a despeito de constituir uma evolução do direito à privacidade, com este não se confunde, sendo, assim, direitos autônomos, cujos objetos de proteção, apesar de muitas vezes se aproximarem, não se confundem, impondo aquele uma proteção estática, negativa, enquanto este impõe uma proteção dinâmica, positiva.

Os casos *National Data Center*, SAFARI e censo alemão, são expressivos quanto ao fomento do debate sobre a proteção dos dados pessoais.

No caso *National Data Center*, o órgão administrativo *Bureau of Budget* americano, pretendia, por volta de 1965, criar uma central nacional para armazenamento de informações pessoais, com o objetivo de centralizar, em único local, as informações sobre os cidadãos americanos que se encontravam dispersas em diversos órgão da administração.

A pretensão despertou diversos debates na sociedade americana, sobretudo diante do "[...] receio generalizado de que a concentração de dados nas mãos da administração pública implicasse no excessivo crescimento de poder do governo, em afronta à tradição liberal da democracia norte-americana" (DONEDA, 2019, p. 161).

As discussões levaram o Congresso a promover audiências públicas, cujos debates ensejaram interessantes conclusões, como no sentido de que, a despeito de uma centralização ser mais benéfica sob o ponto de vista administrativo, a distribuição dos dados pessoais parecia ser mais benéfica ao cidadão; também, no sentido de que as diversas informações pessoais possuem diferentes relevâncias, de modo a merecerem diferentes proteções (DONEDA, 2019, p. 162-163).

O projeto foi descartado após esse intenso debate, todavia, foi qualificado como "vitória de Pirro", porque o referido debate não evoluiu para uma tentativa de regulação do tratamento dos dados sensíveis ou sobre a necessidade governamental quanto ao tratamento das informações pessoais e relativas à privacidade (DONEDA, 2019, p. 163).

No mesmo sentido, no início da década de 1970, o *Instituit National de la Statistique* idealizou publicamente o denominado SAFARI, *Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*, com o objetivo de promover a transferência dos dados pessoais de cidadão francesas para um sistema informatizado vinculado à administração pública.

Igualmente ao ocorrido nos Estados Unidos, o SAFARI foi rejeitado pela opinião pública: “[...] a imprensa francesa publicou artigo a respeito que se tornou célebre, intitulado ‘Safari, ou a caça aos franceses’” (DONEDA, 2019, p. 164).

Resultado da comoção pública foi a interdição, pelo então ministro francês, de qualquer compartilhamento de dados entre os ministérios, cujo efeito prático foi o encerramento do SAFARI. Todavia, diferentemente do ocorrido nos Estados Unidos, os debates sobre o SAFARI levaram à criação da comissão *Informatique et Libertés*, do que resultou a lei francesa de proteção de dados pessoais de 1978 (DONEDA, 2019, p. 165).

O caso do censo alemão diz respeito aos trabalhos do censo desenvolvidos pela Alemanha, que deveria findar em 1983, os quais, porém, despertaram forte desconfiança pela sociedade alemã quanto ao método de coleta e quanto ao destino dessas informações.

Aprovada em 1982, a lei do censo detinha vários pontos controversos. Previa: 160 perguntas a serem respondidas, as quais seriam posteriormente submetidas a tratamento informatizado; a possibilidade de confronto das informações com outras constantes do registro civil, a fim de potencialmente promover a alteração do próprio registro; a possibilidade de transmissão desses dados, desde que sem identificação por nome, aos estados; uma multa pecuniária como punição aos que não respondessem ao questionário, e um mecanismo para favorecer aqueles que denunciassem os que não respondessem ao questionário (DONEDA, p. 165-166).

Referida lei foi alvo de diversos questionamentos, devido aos relevantes aspectos polêmicos mencionados que ensejaram o sentimento de insegurança na população “[...] aliado à impressão de que o governo poderia se valer dos dados obtidos – que, a princípio, serviriam a finalidades estatísticas – para realizar um controle capilar das atividades e da condição pessoal dos cidadãos” (DONEDA, 2019, p. 166).

O desfecho do caso foi o julgamento pela inconstitucionalidade da lei do censo, pela Corte Constitucional alemã. A célebre sentença definiu conceitos essenciais à compreensão da proteção de dados pessoais em todos os ordenamentos jurídicos mundo afora: definiu o hoje entendido como princípio da finalidade, ao enunciar que a lei não poderia utilizar os dados recolhidos para fins diversos dos estatísticos; desmistificou a noção de que existiriam dados pessoais irrelevantes, dando importância a todo e qualquer dado pessoal; definiu a expressão

“autodeterminação informativa”, compreendida como o direito de os indivíduos “decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados” (DONEDA, 2019, p. 167).

> As consequências da sentença sobre o censo foram claras: uma nova lei, que veio a corrigir os pontos contestados, foi promulgada em 1985 para o censo que foi realizado em 1987. Neste novo censo os dados para fins estatísticos eram separados das informações individuais; o cidadão era cuidadosamente informado sobre as finalidades da coleta de informações e sobre sua obrigação de fornecê-las; a transferência de dados pessoais entre autoridades federais e regionais foi simplesmente vetada; entre diversas outras disposições (DONEDA, 2019, p. 168).

Referidos casos enunciam expressivos momentos históricos que fomentaram intenso debate acerca da proteção dos dados pessoais, comumente registrados nas doutrinas especializadas como marcos históricos fundamentais à compreensão da temática.

A par desses emblemáticos casos relativos à proteção de dados pessoais, também se desenvolviam legislações específicas sobre a matéria, cujo início se deu na década de 1970. A especializada doutrina de Doneda (2019, p. 174-179), trata das gerações de leis de proteção de dados pessoais.

A primeira geração se caracteriza por leis relativas à criação de bancos de dados e respectivo controle pelas administrações públicas com ênfase no controle de informações pessoais pelo Estado, verdadeiros protagonistas da criação dessas leis (DONEDA, 2019, p. 174-176).

Pode-se citar a Lei do *Land* alemão de Hesse, de 1970, a qual criou uma autoridade de proteção de dados com o objetivo de controlar a elaboração informática de dados pessoais na perspectiva da administração pública. Em 1973 surge na Suécia, a primeira lei nacional de proteção de dados, o “Estatuto para bancos de dados de 1973”, criando também o denominado “inspetor para o uso de dados pessoais”. Também se pode mencionar *Privacy Act* norte-americano de 1974 (DONEDA, 2019, p. 174-175).

A segunda geração de leis sobre proteção de dados pessoais surge desde a metade da década de 1970, esta agora não focada mais especificamente no fenômeno computacional, mas centrada na relevância da privacidade e da proteção dos dados pessoais sob uma perspectiva de liberdade negativa, em que o cidadão se

insere com maior protagonismo a fim de exercer essa liberdade negativa. Pode-se mencionar a lei austríaca de 1978 (DONEDA, p. 176-177).

Nesse mesmo contexto da segunda geração de leis, a despeito de antecederem um regramento específico infraconstitucional, as constituições portuguesa e espanhola trouxeram em seu corpo normas específicas sobre a produção de dados pessoais.

Promulgada em 1976, a constituição portuguesa foi o primeiro texto jurídico que abordou a temática da proteção de dados pessoais de forma sistematizada, em seu artigo 35.º. Muito embora ainda que vinculando o tema a questões informáticas, o referido dispositivo consagrou direito aos titulares de dados, protegendo assim os dados pessoais, o acesso à informação, o acesso aos dados pessoais e à retificação (SALDANHA, 2018, p. 9).

A constituição espanhola de 1978 em seus Arts. 18 e 105, estabeleceu também garantias referentes à privacidade e proteção dos dados pessoais, mencionando especificamente o direito de acesso aos dados pessoais.

A terceira geração de leis nasce na década de 1980 e evolui, assim, para, ainda que do mesmo modo centrada no cidadão, ultrapassar a simples liberdade de o cidadão autorizar ou não o tratamento de seus dados pessoais, de modo a ocupar-se em garantir a efetividade desta liberdade: “As leis de terceira geração encaravam a participação do cidadão como a mola propulsora de sua estrutura” (DONEDA, 2019, p.178).

> O marco destas leis de terceira geração é a decisão do Tribunal Constitucional Alemão, [...] à qual seguiram-se emendas às leis de proteção de dados na Alemanha e na Áustria, além de leis específicas na Noruega e na Finlândia (DONEDA, 2019, p. 179).

Por fim, surgem as leis de quarta geração, cujo conteúdo corresponde as atuais legislações sobre proteção de dados pessoais. O que caracteriza referida geração de leis é o objetivo de superar as desvantagens do enfoque individual dado às gerações de leis anteriores, de maneira a focar uma percepção coletiva sobre a proteção de dados pessoais (DONEDA, 2019, p. 179)

> Entre as técnicas utilizadas, estas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação, que não era resolvido com medidas que simplesmente reconheciam o direito à autodeterminação informativa; outra, paradoxalmente, é a própria redução do papel da decisão individual de autodeterminação informativa. Isto ocorre por que se parte do pressuposto de que

> determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, à qual não pode ser conferida exclusivamente a uma decisão individual (DONEDA, 2019, p.179).

Ainda quanto à evolução de normas a respeito da proteção de dados pessoais, é essencial apontar que em 28 de janeiro de 1981, o Conselho Europeu para proteção de dados pessoais ratificou a Convenção 108, referente ao tratamento automatizado de dados pessoais.

Prevendo garantias sobre dados pessoais sensíveis (raça, opinião política, saúde, convicções religiosas, vida sexual e registro criminal), a Convenção 108 se aplica às atividades de tratamento tanto no setor privado quanto público, com o objetivo de proteger o cidadão diante da coleta do tratamento de seus dados pessoais, e regula, ainda, a transferência internacional dos dados pessoais (SALDANHA, 2018, p. 4).

De forma pioneira, assim, considera-se: a necessidade de tratamento dos dados pessoais de forma íntegra e lícita; que deve haver legitimidade para o armazenamento dos dados pessoais; a compatibilidade para a coleta e para a conservação dos dados pessoais por certo tempo; a exatidão dos dados pessoais e a possibilidade de retificação (SALDANHA, 2018, p. 4).

A isso se seguiu, nos finais da década de 1980, um desejo cada vez maior de a Comissão Europeia harmonizar as leis dos estados-membro da União Europeia, de modo a estimular os países que não tivessem disposições sobre proteção de dados a adotarem legislações relevantes quanto ao tema, na época, como a Itália, Espanha e Grécia (DOVE, 2018, p. 1015).

Nesse sentido, tanto para harmonizar as liberdades fundamentais dos cidadãos europeus em relação ao tratamento de dados, quanto para promover a livre transferência de dados pessoais, veio à tona a Diretiva de Proteção de Dados 46/95 (DOVE, 2018, p. 1015), “como referido pelo Tribunal de Justiça da União Europeia (TJUE), *tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais*” (SALDANHA, 2018, p. 4).

Pode-se dizer que a Diretiva 46/95 constitui um marco do reconhecimento da proteção de dados pessoais como um direito independente (TEJEDOR et al., 2018, p. 26). No direito da União Europeia, foi o primeiro instrumento jurídico referente à

proteção dos dados pessoais e à livre transferência desses dados (SALDANHA, 2018, p. 4).

A referida Diretiva exigia que os estados-membro da União Europeia transpusessem as previsões da Diretiva em sua respectiva legislação nacional, cabendo, porém, a cada país, decidir como alcançar os objetivos estabelecidos pela Diretiva, o que, de um lado, constituiu uma vantagem, permitindo a adaptação às características de cada estado-membro, todavia, também se caracterizou como uma desvantagem, por permitir a realização de manobras que prejudicassem, dessa forma, o principal propósito de harmonização das legislações (DOVE, 2018, p. 1015).

Nesse sentido, no final dos anos 2000, havia ficado clara a perda de relevância da Diretiva 46/95, tanto diante da nova era das tecnologias digitais quanto devido à fragmentação das legislações nacionais, com diferentes níveis de proteção em relação aos dados pessoais, gerando insegurança jurídica e a percepção dos elevados riscos para a proteção dos dados pessoais (DOVE, 2018, p. 1015).

Assim, havia uma preocupação de que os diferentes níveis de proteção em cada país pudessem impedir a livre transferência de dados pessoais, podendo, portanto, promover óbices às relações econômicas entre os países da União Europeia, bem como a possibilidade de concorrência desleal e, também, a possibilidade de isentar autoridades em relação à observância da legislação da União Europeia (DOVE, 2018, p. 1015).

Nesse sentido, em 25 de janeiro de 2012, a Comissão Europeia propõe uma ampla reforma na Diretiva 46/95, a fim de fortalecer a proteção à privacidade e fomentar a economia digital na Europa, do que resultou a aprovação da hoje conhecida GDPR, em inglês, *General Data Protection Regulation*, ou o RGPD, Regulamento Geral de Proteção de Dados, nº 2016/679, aprovado em 27 de abril de 2016.

A GDPR, nesse sentido, ampliou o direito à proteção dos dados pessoais, alargando as garantias dos indivíduos, titulares de dados, nele denominados *data subjects*, com o objetivo de adequar a legislação europeia para a nova realidade da economia da informação, e afastar as lacunas protetivas sob a vigência da Diretiva 46/95.

Por exemplo: a GDPR aumenta o seu âmbito territorial de incidência ao se aplicar ao tratamento de dados realizado pelos agentes que tratam dados de titulares de dados na Europa, independentemente de o controlador ou o operador de dados

estar estabelecido na Europa; quanto à principiologia, se assemelha à Diretiva, porém, há diferenças, como a expressa previsão do tratamento de dados de forma transparente, enquanto a Diretiva previa a transparência de forma implícita (VOSS, 2017, p. 223); cria diversos novos direitos aos titulares de dados, além daqueles previstos na Diretiva, como o direito ao esquecimento ou a alternativa a este, o direito à restrição quanto ao tratamento de dados pessoais (VOSS, 2017, p. 226).

A GDPR tem amplo âmbito de aplicação e ressalta no decorrer de seus considerandos a importância da aplicação uniforme com o objetivo de afastar a fragmentação antes trazida pela Diretiva 46/95, daí porque a sua relevância enquanto um instrumento normativo para regular a proteção dos dados pessoais (TEJEDOR et al, 2018, p. 28).

O Considerando 8 do GDPR, para esse propósito, admite a repetição do texto do GDPR nos ordenamentos jurídicos nacionais somente em situações restritas, isso para que a interpretação sobre o GDPR seja dada apenas pelos Tribunais europeus e não pelos legisladores nacionais, atribuindo, assim, aos estados-membros a restrição ou ampliação das normas do GDPR, sem contrariá-las, de maneira a adequá-las às respectivas realidades nacionais (TEJEDOR et al, 2018, p. 28).

É esta, portanto, a linha histórica, em geral, da proteção de dados pessoais na Europa, sendo o GDPR a grande influência que levou à aprovação da LGPD no Brasil, em um contexto de interesse econômico, inclusive, vale ressaltar.

Antes de se abordar de maneira específica a LGPD, para, então, se passar à análise da figura do DPO, necessário apontar que a LGPD não se trata do primeiro instrumento de proteção de dados pessoais na legislação brasileira.

Isso porque, anteriormente à LGPD, previsões constitucionais e infraconstitucionais já protegiam os dados pessoais em território nacional, em normas esparsas, específicas para relações jurídicas delineadas, em contraponto com a LGPD, que como uma lei “geral”, abrange as relações jurídicas de forma ampla. Cabe citar as principais disposições normativas.

Dessa forma, é imprescindível pontuar que antes mesmo de se pensar em legislação infraconstitucional relativa à proteção de dados pessoais, a própria CF prevê garantias quanto aos dados pessoais.

O *habeas data*, inserido no Art. 5º, inciso LXXII, é um expressivo remédio constitucional que visa a proteção de dados pessoais e a sua atual previsão na CF reflete a experiência constitucional anterior, tendo em vista que nesta era constante o

arquivamento de dados sobre convicção filosófica, política, religiosa e sobre conduta pessoal dos cidadãos, a critério do governo, que o fazia inclusive sigilosamente, de modo que esse remédio se caracteriza como uma insurgência contra órgãos de informação (TEMER, 1993, p. 203).

Pode-se conceder *habeas data*, primeiro, para "[...] assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público" (BRASIL, 1988).

Verifica-se, portanto, a previsão constitucional dos princípios de transparência e livre acesso, que posteriormente vieram a ser dispostos na LGPD, em seu Art. 6º, incisos IV e VI (BRASIL, 2018). E, também previstos na LGPD como direitos dos titulares, é possível anotar a correspondência com os direitos de confirmação da existência do tratamento, acesso aos dados e informação sobre o tratamento de dados, nos termos do Art. 18, incisos I, II e VII (BRASIL, 2018).

Relevante ponderar que o conteúdo da proteção de acesso às informações objetiva não só o acesso e a transparência quanto aos dados constantes de dados públicos em órgãos públicos, mas também se estende a bancos de dados que tenham caráter público, ainda que sejam privados, por exemplo, o cadastro do Serviço de Proteção ao crédito (ARAÚJO; NUNES JÚNIOR, 2005, p. 195).

O *habeas data* é concedido, também, para "[...] retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" (BRASIL, 1988).

No mesmo sentido, a LGPD veio a positivar em nível infraconstitucional o direito de correção de dados incompletos, inexatos ou desatualizados, em seu Art. 18, inciso III (BRASIL, 2018).

Ressalta-se que esta segunda proteção que confere o *habeas data* tem por escopo não só corrigir informações inverdadeiras, mas também poderá solicitar a retificação ainda que diante de uma informação que seja verdadeira, podendo solicitar a sua supressão por meio de tal remédio, desde que essa informação implique violação à lei ou à própria Constituição, por violar a intimidade, por abordar aspectos relativos à condição sexual, por exemplo (ARAÚJO; NUNES JÚNIOR, 2005, p. 196).

Desse modo, "[a]s duas finalidades do *habeas data* são, portanto, independentes e autônomas" (ARAÚJO; NUNES JÚNIOR, 2005, p. 198).

Especificamente quanto à proteção de dados, a CF, em seu Art. 5º, inciso XII, dispõe sobre a inviolabilidade das comunicações:

> [...] é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

A CF garante, portanto, a inviolabilidade das comunicações, e menciona expressamente a inviolabilidade “de dados”, o que se excetua somente em circunstâncias previstas em lei cujo fim seja delimitado à investigação e instrução processual penal. A norma, ao se dedicar ao sigilo das comunicações, tem por escopo proteger exatamente o teor do diálogo e da troca de informações (ARAÚJO; NUNES JÚNIOR, 2005, p. 146), quer dizer, “[...] a Constituição está proibindo que se abram cartas e outras formas de correspondência escrita, se interrompa seu curso e se escutem e interceptem telefonemas” (SILVA, 2007, p. 104).

O CDC (Código de Defesa do Consumidor) é sempre mencionado na literatura especializada como um importante marco de proteção de dados pessoais, então, na esfera consumerista, ao dispor em seus Arts. 43 e 44 regramento direcionado à proteção dos consumidores frente a bancos de dados e cadastros de consumidores (BRASIL, 1990).

Importante mencionar que, quando o CDC separa as figuras dos “bancos de dados” e dos “cadastros de consumidores”, quer dar exatamente diferentes significados, de modo que, quanto ao primeiro, se refere ao conjunto de informações que objetivam fazer análise de crédito, baseadas, primordialmente, em dados financeiros e patrimoniais; e quanto ao segundo, se refere à conjunção de dados para fins de gerir as informações para finalidades específicas do fornecedor, por exemplo, para gerir os consumidores por categorias que permitam a participação ou não de ofertas promocionais (ARAÚJO, 2017).

O interessante para este trabalho é que nos Arts. 43 e 44 o CDC conferiu proteção muito específica aos consumidores, garantindo nessa seara normativa, com muita clareza direitos que vieram a ser consolidados na LGPD, tais como os direitos de acesso e de retificação, dispostos no Art. 18, incisos II e III e LGPD, e previu, também, o princípio da transparência, positivado, agora no Art. 6º, inciso VI, da LGPD (BRASIL, 2018).

A chamada Lei de Acesso à Informação, Lei 12.527 de 2011, também é vista como um importante instrumento que regulamentou expressamente a proteção de dados pessoais em nível infraconstitucional. Em seu Capítulo IV, aborda

expressamente na Seção V, denominada “Das Informações Pessoais”, sobre a proteção de dados pessoais, cuja preservação é pretendida em contraponto com a transparência que visa dar a Lei às informações públicas, conforme dispõe o *caput* do Art. 31: “[o] tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, à vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais” (BRASIL, 2011).

O que a Lei de Acesso à Informação fez, portanto, foi trazer a proteção dos dados pessoais como um balizador da transparência objetivada.

Indispensável, ainda nessa retrospectiva, mencionar que o Marco Civil da Internet, Lei 12.965 de 2014, recepcionou de forma expressa, como um princípio, a proteção dos dados pessoais, em seu Art. 3º, inciso III (BRASIL, 2014).

Especificamente no Capítulo II, o MCI (Marco Civil da Internet) traz regras específicas sobre a proteção dos dados pessoais no âmbito da internet.

Nesse sentido, o MCI trouxe como direitos dos usuários a inviolabilidade e o sigilo do fluxo das comunicações por meio da internet e das comunicações privadas armazenadas, o direito à transparência quanto à forma de proteção de registros de conexão e de acesso a aplicações, o direito à proteção dos dados pessoais contra terceiros, salvo se permitido mediante consentimento livre, expresso e informado (BRASIL, 2014).

De suma relevância compreender que o MCI consagrou desde então o princípio da finalidade, ao prever que o tratamento dos dados pessoais tão somente pode ser realizado para as situações em que haja justificativa para a coleta, que não haja vedação em Lei, e desde que haja específica previsão em contrato ou em termos de uso de aplicações na internet (BRASIL, 2014).

Ademais, também previu como um direito dos usuários, no Art. 7º, inciso IX, o “consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais” (BRASIL, 2014).

E ainda, o MCI garantiu o direito à exclusão dos dados pessoais que os usuários forneçam a aplicações de internet desde que o requeira, após o fim da relação entre as partes, ressalvando-se as hipóteses em que o provedor, por obrigação legal, deve manter a guarda dos registros (BRASIL, 2014).

O que fica claro, portanto, e de relevância a este trabalho, é que o MCI regulamentou, com certa especificidade, inclusive, a proteção dos dados pessoais no

âmbito da internet, consagrando-se, dessa forma, como uma Lei setorial sobre proteção de dados pessoais que antecede e reforça a necessidade de uma proteção geral de dados, amplificada e aplicável a todos os tipos de relações, como é a LGPD.

É de se concluir, nesse sentido, que o debate e o regramento da proteção de dados pessoais é de longa data, podendo-se notar a sua evolução legislativa no mundo, de forma expressa, desde a década de 1970.

No Brasil, no atual panorama jurídico-normativo, a proteção de dados pessoais encontra respaldo de forma expressa por meio do remédio do *habeas data*, afora a proteção conferida pelo CDC, pela Lei de Acesso à Informação, e o notável regramento específico conferido pelo MCI quanto ao tratamento de dados no âmbito da internet.

Desse modo, a LGPD corrobora as previsões normativas brasileiras e amplia a proteção, em consonância com o movimento normativo interno e, seguindo (porque atrás), o panorama mundial relativo à proteção de dados pessoais, mormente após a edição da GDPR, que impôs, inclusive por fatores relativos à manutenção das relações econômicas, a aceleração de um regramento com garantias equitativas quanto à proteção dos dados pessoais no Brasil.

Neste primeiro capítulo, portanto, se examina todo o contexto em que a LGPD se insere. Verifica-se a ruptura do padrão econômico, de maneira que a informação se torna um bem de valor, a assumirem papel central as tecnologias da informação, e a ocorrer a mudança dos bens de consumo materiais para os digitais. O direito à privacidade surge como resposta, cada vez mais robusta conforme evolui essa nova econômica e os seus produtos tecnológicos. E, então, o direito à proteção de dados pessoais, além da privacidade, busca proteger, de maneira específica, os seus titulares, cujos instrumentos normativos têm evoluído de maneira constante para amplificar e coletivizar essa proteção.

Resultado, portanto, de todo esse processo abordado do presente capítulo, a LGPD é examinada no capítulo a seguir em seus principais aspectos, conforme o recorte metodológico desta pesquisa, para permitir, no terceiro capítulo a compreensão da moldura jurídica que envolve a figura do DPO.

3 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Após indicar a proteção aos dados pessoais conferida por instrumentos como o *habeas data*, o sigilo de dados de comunicações, a lei do cadastro positivo, e as previsões do CDC quanto aos bancos de dados, Cueva (2017) alertou sobre a necessidade de um marco legal sobre a proteção dos dados pessoais no Brasil: “[a] edição de lei nacional de proteção dos dados pessoais é essencial para suprir as omissões hoje existentes e garantir um nível adequado de proteção”.

Como apontado no capítulo anterior, o que se viu no ordenamento jurídico brasileiro antes da LGPD foram previsões normativas esparsas que conferiam proteção aos dados pessoais em situações específicas.

O cenário normativo no Brasil quanto à proteção de dados pessoais mais tinha lacunas do que previsões legislativas, fazendo da edição de uma Lei abrangente sobre o tema uma necessidade irremediável.

De outro lado, em abril de 2016 foi aprovada a GDPR na União Europeia, conforme estudado anteriormente, regulamento este que veio para dirimir as dissonâncias entre as legislações nacionais dos países integrantes da União Europeia, de modo a dar maior segurança jurídica às relações e garantir o desenvolvimento econômico, sobretudo nos ambientes digitais.

A GDPR entrou em vigor em 25 de maio de 2018 e teve impacto decisivo para a aprovação da LGPD no Brasil. Tanto é que a LGPD foi aprovada em menos de três meses após o início da vigência da GDPR, em 14 de agosto de 2018.

Duas circunstâncias foram fundamentais para que a GDPR tivesse esse efeito sobre a vontade legislativa do Brasil.

Primeiro é o fato de que a GDPR abordou de forma ampla os agentes de tratamento sujeitos ao seu regramento, de forma que os agentes de tratamento ainda que ajam em território estrangeiro ou sejam estrangeiros, na hipótese em que ofereçam bens ou serviços ou realizem atividades de *profiling* relacionadas a pessoas que estejam na União Europeia, estão obrigados à observância da GDPR (MALDONADO, 2019, p. 14).

Em segundo lugar, a GDPR determinou que quaisquer transferências internacionais de dados pessoais devem ser realizadas entre agentes de tratamento cujo país adote garantias equivalentes às previstas na GDPR (MALDONADO, 2019, p. 14).

Por essas razões, sob pena de se restringir abruptamente as relações comerciais entre Brasil e União Europeia é que houve grande celeridade para amplificar a proteção de dados pessoais em território nacional, a se buscar, inclusive, uma equivalência mínima de proteção com a GDPR (MALDONADO, 2019, p. 14).

Assim, foi aprovada a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

Aprovada sem regramento específico sobre a Autoridade Nacional de Proteção de Dados (ANPD), a LGPD foi objeto de alteração da Medida Provisória nº 869 de 2018, posteriormente transformada na Lei nº 13.853 de 2019, a fim de criar a ANPD, e terminou por promover, também, alterações normativas pontuais.

Nesse sentido, a LGPD dispõe em seu Art. 1º sobre o seu objeto de incidência, de modo a normatizar que o seu regramento recai sobre o tratamento de dados pessoais, sendo clara quanto à abrangência tanto de meios físicos quanto dos meios digitais, a sujeitar às suas disposições as pessoas naturais e jurídicas, de direito público ou privado (BRASIL, 2018).

Relevante ponderar que ao tecer sobre o seu objeto de incidência, o Art. 1º expressa que o objetivo da lei é “[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

A consignação dos direitos de liberdade e de livre desenvolvimento da personalidade da pessoa natural vão ao encontro de relevante parte da doutrina acerca da compreensão do conteúdo do direito à proteção dos dados pessoais, na medida em que a liberdade e o desenvolvimento da personalidade de forma livre são vistos como consequências a serem garantidas por meio dos regramentos específicos de proteção de dados pessoais.

É dizer, para que o indivíduo seja livre e se desenvolva livremente é preciso que lhe seja garantido que seus dados pessoais não serão tratados de modo a comprometer ou interferir em sua liberdade de escolha.

Quando se refere à privacidade, não destoa a LGPD do sentido conferido ao direito à proteção de dados pessoais, mas busca preservar referida proteção naquilo em que é cabível se falar de privacidade no âmbito dos dados pessoais, sem excluir o entendimento respeitante às normas de proteção de dados que extrapolam o sentido da dicotomia entre público e privado.

Outrossim, neste capítulo serão analisados os fundamentos e princípios da LGPD, os direitos dos titulares, as bases legais de tratamento, as boas práticas e, por fim, se abordará as regras atinentes à ANPD, temas estes fundamentais para compreender a figura do DPO, porquanto este deve agir como intermediário entre os agentes de tratamento e os titulares de dados e entre aqueles e a ANPD.

Aponta-se que se faz a escolha de não enveredar este trabalho no estudo dos conceitos previstos no Art. 5º da LGPD, tendo em vista que a previsão legal é autoexplicativa, ainda que em certa medida, remetendo-se o leitor à leitura dos conceitos da LGPD na hipótese em que se faça necessário a compreender quaisquer conclusões desta pesquisa.

Ato seguinte, passa-se à análise dos fundamentos da LGPD.

3.1 Fundamentos

A LGPD traz os seus fundamentos no Art. 2º. Como primeiro fundamento, o inciso I estabelece o respeito à privacidade. Visto outrora, o direito à proteção dos dados pessoais a despeito de abranger outras esferas atualmente, decorre historicamente e metodologicamente do direito à privacidade, sendo, portanto, deste, em certa medida, indissociável.

Tendo em vista que tudo o que o indivíduo faz pode ser objeto de registro e que esses dados podem ser compilados, organizados, analisados por pessoas ou por robôs, faz todo sentido se falar em privacidade não só como o embrião do direito à proteção dos dados pessoais, mas como um elemento que o permeia.

Conforme ensina Vainzof (2019, p. 26):

> O cruzamento de dados pessoais cadastrais, análises de comportamento em redes sociais, compras com cartão de credito, tempo de permanência em páginas da internet, meros registros de acesso a aplicações, informações de geolocalização ou de consumo de energia podem estabelecer parâmetros fidedignos para identificar e traçar perfis consistentes de indivíduos, seus gostos e interesses, seja para direcionar um produto ou serviço, para validar uma contratação profissional, seja para identificar um potencial criminoso.

Veja-se, assim, que falar em proteção de dados pessoais implica também o direito à privacidade. Demais considerações histórico-evolutivas, inclusive sobre a legislação nacional tocante à privacidade estão dispostas no capítulo anterior, em que há aprofundamento sobre o tema.

Seguindo-se, a autodeterminação informativa é o segundo fundamento elencado no Art. 2º, inciso II. O direito à autodeterminação informativa confere ao titular de dados o poder de controle das informações que lhes são pessoais, é dizer, dá ao titular de dados o direito subjetivo de decidir, nos limites da lei, o que, como, quando, por quem e de que forma serão tratados seus dados pessoais.

Assinalado na primeira seção desta pesquisa, os dados são o novo petróleo, de maneira que, quanto maior o volume de dados que uma determinada organização possui, maior é o seu valor, a exemplo da aquisição do *WhatsApp* pela *Facebook Inc.*, transação em que a empresa foi adquirida por US$ 22 bilhões a despeito de ter tido um prejuízo no ano anterior de US$ 130 milhões (BARIFOUSE, 2018).

Nesse sentido, o direito à autodeterminação informativa devolve aos indivíduos, aos titulares de dados, o controle sobre os seus próprios dados pessoais neste cenário em que a economia da informação provoca uma verdadeira voracidade dos agentes econômicos quanto ao tratamento dos dados pessoais a fim de gerar valor às empresas.

Nesse novo contexto da economia da informação em que os dados são extremamente valiosos, Rodotà (2008, p. 113) muito bem explica que “[...] a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações”.

A despeito do amplo debate que o atual cenário da economia da informação provoca, o direito à autodeterminação informativa não se trata de uma novidade trazida pela LGPD nem pela GDPR, mas foi consagrado pelo Tribunal Constitucional Federal da Alemanha no julgamento sobre a constitucionalidade da lei do censo alemã de 1982.

Ao julgar pela inconstitucionalidade da lei do censo, a decisão definiu conceitos essenciais à compreensão da proteção de dados pessoais: definiu o hoje entendido como princípio da finalidade, ao enunciar que a lei não poderia utilizar os dados recolhidos para fins diversos dos estatísticos; desmistificou a noção de que existiriam dados pessoais irrelevantes, dando importância a todo e qualquer dado pessoal; definiu a expressão “autodeterminação informativa”, compreendida como o direito de os indivíduos “decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados” (DONEDA, 2019, p. 167).

Segundo reconheceu expressamente a Corte Alemã, o direito à autodeterminação informativa quer significar que: “o indivíduo exerça sua liberdade de decisão sobre as ações a serem precedidas ou omitidas em relação a seus dados” (VIEIRA, 2007, p. 88).

Daí que se pode indicar que o conteúdo do fundamento da “autodeterminação informativa” fornece elementos para embasar a proteção de dados pessoais também no direito à liberdade. Do que se observa até aqui, o direito à privacidade e o direito à proteção dos dados pessoais são distintos e, a despeito de a proteção dos dados pessoais poder encontrar substrato no direto à privacidade, por com aquele ter pontos de contato, também é fundamentada no direito à liberdade por buscar garantir ao titular de dados, como apontou Doneda (2019, p. 167), que possam decidir “por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados” (DONEDA, 2019, p. 167).

O direito à liberdade é notoriamente consagrado no ordenamento jurídico brasileiro como um direito fundamental, no *caput* do Art. 5º da CF. E, desse modo, sustenta que os titulares de dados têm a liberdade de decidir sob quaisquer ângulos acerca do tratamento de seus dados pessoais (dentro dos limites legais). A autodeterminação informativa, portanto, pode ser depreendida do direito fundamental à liberdade.

Nesse sentido, é interessante rememorar que o direito à privacidade se caracterizaria por uma lógica *negativa*, sendo que, de outro lado, ao se tratar de proteção de dados pessoais, a lógica seria *positiva*.

Disso pode-se verificar que, se tratando de direito à privacidade, há encontro com o direito à liberdade de maneira negativa. Quer dizer, se a privacidade consiste no direito de ser deixado em paz, de estar só, de o indivíduo não sofrer ingerências na sua vida privada e íntima, encontra contato com o direito à liberdade no sentido de que lhe seja garantida a liberdade e negar qualquer ingerência em sua vida íntima e privada.

De outro lado, o direito à proteção de dados também se sustenta na liberdade, porém, sob uma perspectiva *positiva* e, ao se observar o fundamento da autodeterminação informativa, como a garantia ao titular de dados de determinar sob diversas perspectivas o tratamento de seus dados pessoais.

Seguindo-se, note-se que é do direito à autodeterminação informativa que se extrai todos os direitos dos titulares de dados previstos na LGPD. Portanto, a

autodeterminação informativa é um chamariz que sustenta todos os direitos dos titulares de dados dispostos no Art. 18 da LGPD. Ora, o titular de dados tem direito de acesso porque tem o poder de controlar se os agentes podem ou não acessar seus dados. Tem o direito de retificação porque tem o poder de garantir que seus dados pessoais expressem a verdade. Tem o direito de exigir a eliminação porque tem o poder de determinar que um agente deixe de tratar os seus dados se não possuir nenhuma base legal que o autorize. Ou seja, todos os direitos do titular de dados são instrumentos para fazer concretizar o fundamento da autodeterminação informativa.

Como terceiro fundamento, o inciso III aborda a liberdade de expressão, de informação, de comunicação e de opinião. A pretensão da LGPD é garantir a liberdade do titular de dados em todas as suas formas e ainda não fazer de suas previsões um meio para restringi-las.

A liberdade de expressão e de opinião, constitui um direito fundamental previsto no Art. 5º, inciso IV da CF, de modo que, ainda que não estivesse expressa na LGPD, por se tratar de garantia disposta na Carta Magna de qualquer modo regeria as relações que envolvam proteção de dados pessoais.

Por sua vez, a prevista liberdade de informação pretende assegurar que as informações aos indivíduos não sejam restringidas. Aqui é oportuno reiterar a situação já vista referente aos filtros bolha, em que há a customização das informações entregues aos usuários (MAGRANI, 2014, p. 118), o que é feito com base nos dados tratados dos próprios usuários, situação essa a ser rechaçada por meio da correta aplicação da liberdade de informação. A liberdade de comunicação também encontra resguardo na CF, Art. 5º, inciso XII, na medida em que o seu sigilo é inviolável, salvo hipóteses excepcionais.

Por sua vez, a inviolabilidade da intimidade, da honra e da imagem constituem o quarto fundamento, nos termos no Art. 2º, inciso IV. A intimidade aqui deve ser compreendida como uma das esferas da privacidade conforme norteia a literatura jurídica especializada. Intimidade, honra e imagem também estão consignadas como direito fundamental do Art. 5º, inciso X da CF.

O que se observa é que a LGPD buscou reforçar a proteção a referidos direitos, em especial a intimidade que foi disposta de maneira separada da privacidade com o claro escopo de diferenciá-las, tratando-se a intimidade dentro do aspecto mais restrito da vida privada ao qual a LGPD deu relevância.

A LGPD está fundada, também, no desenvolvimento econômico e tecnológico e na inovação. É sobre o que trata o inciso V do Art. 2º. Como uma economia de mercado que é o sistema econômico brasileiro, o desenvolvimento econômico baseado em pesquisa lhe é intrínseco. Não à toa, a CF prevê em seu Art. 218 que: "[o] Estado promoverá e incentivará o desenvolvimento cientifico, a pesquisa, a capacitação cientifica e tecnológica e a inovação" (BRASIL, 1988).

O que pretende a LGPD, portanto, é garantir que a proteção conferida aos dados pessoais não só não constitua um empecilho para a economia, a tecnologia e a inovação, mas, também, que o seu próprio corpo normativo seja fomento para fazer realizar os objetivos econômicos, tecnológicos e de inovação, delineados pelo Estado.

> Assim, é natural que a disciplina imposta pela LGPD não deve, a não ser em casos excepcionais, piorar ou impedir o perfeito desempenho do Estado na realização de seus interesses, e um deles, como visto, é o desenvolvimento econômico, tecnológico e a inovação (COTS; OLIVEIRA, 2018, p. 72).

Portanto, tal inciso reforça um mandamento constitucional e assegura o livre desenvolvimento da economia de mercado em todos os seus aspectos, tendo tido o legislador a pretensão de esclarecer que o novo regime jurídico de proteção de dados atuará como fundamento para o desenvolvimento econômico, tecnológico e a inovação, e não como um óbice.

De maneira complementar ao fundamento anterior, a livre concorrência e a defesa do consumidor constituem o conteúdo do inciso VI do Art. 2º. A livre iniciativa configura um dos mecanismos da economia de mercado, de modo a ter por regra a liberdade para que todos os indivíduos possam empreender em todos os setores da economia, de modo que a restrição para o exercício de certas atividades ou profissões se apresenta de forma excepcional. É o que acontece, por exemplo, com certas atividades profissionais, como a advocacia, que demanda o preenchimento de requisitos para o seu exercício.

Por sua vez, a livre concorrência admite que, por regra, os setores do mercado não serão monopolizados a determinados agentes, salvo nos casos em que a própria lei confira de forma excepcional a reserva de setores do mercado. É o que se observa, por exemplo, com o setor de energia elétrica, em que territorialidades são reservadas a agentes exclusivos.

A defesa do consumidor vem a alargar as garantias já preconizadas para as relações de consumo por meio do CDC e, inclusive, por meio do regramento

específico sobre os bancos de dados. Ora, tendo em vista que relevante parte das relações contratuais estabelecidas em sociedade são relações de consumo, certo é que a proteção do consumidor deve nortear qualquer norma de proteção de dados pessoais.

A assertividade de Rodotà exige reiterar a sua leitura sobre o valor dos dados: “a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações” (RODOTÀ, 2008, p. 113).

Nas diuturnas, recorrentes e inúmeras relações contratuais de consumo, acirra-se a coleta de dados para os mais diversos tipos de tratamento, como uma forma de pagamento pelo produto ou serviço e, assim, merecem referidas relações o exato patamar que lhes foi conferido na LGPD.

Como último fundamento, a LGPD apresenta os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, contidos no inciso VII do Art. 2º.

A garantia da proteção à dignidade da pessoa humana é mais que um direito fundamental do sistema constitucional brasileiro, configura fundamento da República conforme Art. 1º, inciso III, da CF. Nesse sentido, relevante ponderar o que assevera a Carta de Direitos Humanos e Princípios para a Internet:

> Todos os indivíduos têm o direito à privacidade online, incluindo o direito de não ser vigiado, o direito de usar criptografia e o direito ao anonimato online. Todos os indivíduos têm também o direito a proteção de dados, incluindo o controle sobre coleta, retenção, tratamento, eliminação e divulgação de dados pessoais (FÓRUM..., 2011).

No mesmo sentido consigna Doneda (2015, p. 370), em defesa da proteção à dignidade e à liberdade de desenvolvimento da personalidade:

> Quando os cidadãos passam a ser cada vez mais avaliados e classificados apenas a partir de informações a seu respeito, a proteção e o cuidado deixam de ser um aspecto que somente diga respeito às esferas do sigilo ou da privacidade, passando a figurar um componente essencial para determinar o grau de liberdade de autodeterminação individual de cada pessoa.

Por conseguinte, o que pretende a LGPD é maximizar em todos os seus aspectos a dignidade da pessoa humana, em consonância com este mesmo fundamento da República, na forma do Art. 1º, inciso III, da CF, e em consonância com o mais moderno entendimento do conceito do direito à proteção de dados

pessoais, ou seja, garantir liberdade, digna, de desenvolvimento da personalidade do indivíduo, protegendo-o, assim, de ingerências externas, por meio de tratamento indesejado de seus dados pessoais.

Todos os fundamentos apresentados demandam exaustivo debate teórico, entretanto, devido ao recorte metodológico desta pesquisa, este trabalho se limita a os expor para efeitos de compreender o papel do DPO frente a tais fundamentos.

Da mesma forma que é relevante aqui indicar os fundamentos, se faz também imprescindível elencar os princípios da proteção de dados pessoais, normas estas diante das quais o DPO deverá ponderar a tomada de decisão, sobretudo quando se observar complexas situações concretas que ainda não foram alvo de decisões judiciais ou administrativas anteriores.

3.2 Princípios

Compreender os princípios que a LGPD elenca é atividade elementar no trato da proteção de dados pessoais, por se referirem às normas gerais e abstratas que ordenam todo o tratamento de dados pessoais, de maneira que os agentes de tratamento devem observar tais princípios do início ao fim do tratamento.

E, nesse sentido, é também atividade diária do DPO pautar as suas orientações pelos princípios da proteção de dados pessoais, a fazer da observância de tais princípios o norte no tratamento dos dados pessoais, inclusive, porque a obediência a tais princípios pode ser exigida por todas as pessoas que têm titularidade para exigir legalidade no tratamento dos dados pessoais, como o Ministério Público, a Defensoria Pública e associações, bem como pela ANPD e ainda os próprios titulares de dados, que, na forma da LGPD podem exercer todos os direitos elencados no Art. 18, aos quais deve responder o agente de tratamento.

Neste ponto é necessário consignar que é adotada a tipologia normativa segundo a teoria dos direitos fundamentais desenvolvida por Robert Alexy: compreende-se que as normas são divididas em regras e princípios. Nessa toada, segundo Alexy (2015, p. 87), “[t]anto regras quanto princípios são normas, porque ambos dizem o que deve ser”.

Os princípios enumerados pela LGPD, portanto, são normas, como todas as demais regras estabelecidas para a proteção de dados pessoais, cuja observância, portanto, é obrigatória em todas as atividades de tratamento, e por todos os seus agentes, a deverem ser objeto de zelo pelo DPO no exercício de suas atividades.

Dessa forma, o Art. 6º da LGPD indica que “[a]s atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios [...]” (BRASIL, 2018).

Antes de entrar, portanto, nos princípios da proteção de dados especificamente, deve-se notar que não só os princípios foram enunciados como normas, mas também o princípio da boa-fé.

A boa-fé a que se refere o *caput* do Art. 6º diz respeito à boa-fé objetiva, à boa-fé contratual. A boa-fé objetiva é uma norma principiológica, tendo, portanto, o condão de reger as relações em sociedade. Dessarte, determina que os indivíduos devem agir conforme o que, objetivamente, se considera enquanto ético, de maneira a repudiar, e consequentemente, tornar ilícita, a conduta que se amoldar ao que objetivamente reputa-se antiético.

A boa-fé objetiva, boa-fé contratual, está expressamente prevista no Código Civil, Art. 422, que literalmente dispõe: “[o]s contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé” (BRASIL, 2002).

Tartuce (2014, p. 88) explica que o conteúdo do Art. 422 significa que em todas as fases do contrato as partes devem agir de forma proba e com lealdade, e assenta, também, que o princípio da boa-fé contratual encontra respaldo constitucional tanto no fundamento da dignidade da pessoa humana, no Art. 1º, inciso II, da CF, quanto no direito de acesso à informação, na forma do Art. 5º, XIV.

Nesse eito, é relevante anotar que o princípio da boa-fé contratual admite cinco desdobramentos, reconhecidos difundidamente pela doutrina e pelos Tribunais brasileiros: *supressio*, *surrectio, tu quoque*, *venire contra factum proprium no potest* e *duty to mitigate the loss*.

A *supressio* trata da perda do direito pelo decurso do tempo por se ter gerado, na outra parte, a expectativa de que tal direito não seria mais exercido, situação esta atrelada a uma relação de confiança que permeia a relação contratual. Quando se opera a *supressio* para a parte que perde o direito, para a outra parte que se beneficia da perda do direito ocorre a *surrectio*, ante a confiança que aquela primeira gerou nesta parte quanto ao seu não exercício.

A *supressio* exige “[...] a constatação de que o comportamento tendente a o exercer é inadmissível, segundo o princípio da boa-fé, uma vez que antagônico à expectativa gerada pelo não exercício anterior” (MELLO, 2015).

Tartuce (2015, p. 96) menciona como exemplo de ocorrência da *supressio* e da *surrectio* a situação em que as partes dispõem contratualmente que o pagamento de uma obrigação será realizado no domicílio do credor, mas que, faticamente, sempre é paga no domicílio do devedor, de sorte que se torna exigível o pagamento no domicílio do devedor, diante a confiança gerada quanto ao pagamento em referido domicílio.

Ainda, o desdobramento *venire contra factum proprium* tem o objetivo de proibir a adoção de comportamentos contraditórios, ou seja, proibir a parte de adotar uma postura por ter gerado na outra, inicialmente, a confiança de que se comportaria de maneira diversa. É a vedação ao comportamento contraditório no contexto das relações contratuais.

Pessoa (2013, p. 60), em trabalho específico sobre o tema, ensina de forma muito lúcida:

> A expressão significa a oposição de "vir contra o fato próprio", mas na compreensão jurídica significa agir contra seus próprios atos. Trata-se da proibição ao comportamento contraditório, numa sequência lógica de dois atos encadeados. Um segundo ato – o *venire* – se mostra incoerente e incompatível (contraditório) com o primeiro – o *factum proprium* –, embora ambos, em linha de princípios, aparentem licitude.

Ou seja, fica vedado o comportamento da parte, muito embora aparente ser lícito, diante da incoerência diante do comportamento expressado anteriormente.

Tartuce (2015, p. 98) leciona que a decisão mais conhecida que expressa a vedação ao comportamento contraditório foi o Recurso Especial nº 1.996/0030416-5, de relatoria do Ministro Ruy Rosado de Aguiar, caso em que o marido realizou um compromisso de compra e venda sem a anuência da esposa (o que seria causa de nulidade absoluta), com o qual informou ter anuído tacitamente a esposa em um processo, posteriormente. Entretanto, após dezessete anos, a esposa pleiteou a declaração de nulidade do contrato, o que foi rechaçado pelo Superior Tribunal de Justiça que reconheceu a impossibilidade de oposição ao pedido de outorga da escritura definitiva com base na *venire contra factum proprium*, por ter entendido se tratar de um comportamento contraditório com a postura anterior (por ter expressado sua anuência tácita), o que, portanto, é vedado pela boa-fé objetiva.

A *tu quoque*, de seu turno, "significa que um contratante que violou uma norma jurídica não poderá, sem a caracterização do abuso de direito, aproveitar-se dessa situação anteriormente criada pelo desrespeito" (TARTUCE, 2013, p. 97). Quer dizer:

a parte que viola uma norma está proibida de tirar algo que estaria sob seu poder ante a norma que ela própria violou.

Tartuce (2013, p. 97), prossegue a explicar, assim, que por meio da *tu quoque* "evita-se que uma pessoa que viole uma norma jurídica possa exercer direito dessa mesma norma inferido ou, especialmente, que possa recorrer, em defesa, a normas que ela própria violou".

Veja-se, nesse sentido, por aplicação da *tu quoque*, que "[o] condômino que viola regra do condomínio e deposita móveis em área de uso comum, ou a destina para uso próprio, não pode exigir do outro comportamento obediente ao preceito" (GONÇALVES, 2012, p. 62).

Por fim, o *duty to mitigate the loss* aponta o dever de a parte credora mitigar, adotar posturas possíveis, para diminuir os seus próprios prejuízos, de modo a violar a boa-fé objetiva, portanto, a conduta do credor que, em situação de inadimplemento, permanece inerte, admitindo que os prejuízos se majorem a despeito de poder agir para diminui-los.

O Enunciado 169 da III Jornada de Direito Civil do Conselho da Justiça Federal, orienta nesse sentido: "[o] princípio da boa-fé objetiva deve levar o credor a evitar o agravamento do próprio prejuízo".

Tartuce (2013, p. 100) demonstra que, no caso de um contrato de locação em que o locatário deixa de pagar os alugueis, pelo *duty to mitigate the loss* é vedado ao locador deixar de pleitear desde logo o despejo, a fim de que a dívida não se eleve excessivamente, e, também, citando o caso de contratos bancários, na situação em que a instituição bancária verifique o inadimplemento, de imediato deve agir para que o débito não assuma valores astronômicos mormente diante das altas taxas de juros permitidas às atividades bancárias, as quais, inclusive, em uma situação como a relatada, poderiam ser substituídas pelos juros legais em virtude da inobservância do *duty to mitigate the loss*, conclusão esta, aliás, a qual chegou o Tribunal de Justiça do Mato Grosso do Sul no julgamento do acórdão 2009.022658-4/0000-00, de relatoria do Desembargador Rubens Bergonzi Bossay.

Em conclusão, quanto ao princípio da boa-fé, trata-se de um princípio que permeia as relações contratuais e que possui diversos desdobramentos que exemplificam a maneira de ser observado.

O Art. 6º da LGPD, nesse sentido, decidiu por aplicá-lo a todas as atividades de tratamento de dados, sejam elas contratuais (o que, evidentemente, será a maioria), sejam elas não contratuais.

Desse modo, o DPO, ao intermediar as relações agente de tratamento-titulares de dados e agentes de tratamento-ANPD e ao zelar pelo lícito tratamento dos dados pessoais, deve zelar pela adoção de posturas de boa-fé, leais e probas, entre todos os sujeitos que envolvam referidas relações, sob pena de haver a prática de ilícito, tendo em vista que a boa-fé constitui um princípio.

Seguindo-se, a LGPD, no Art. 6º, elenca dez princípios específicos referentes ao tratamento de dados, quais sejam: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas (BRASIL, 2018).

Cots e Oliveira (2018, p. 99-100) ressaltam a importância de a LGPD ter trazido, além de suas regras específicas, os princípios que devem nortear todo o tratamento de dados pessoais, tendo em vista o risco de as regras se tornarem obsoletas diante de atividades tão dinâmicas, mutáveis, que envolvem o tratamento de dados pessoais, de maneira que, com o estabelecimento dos princípios, evita-se a prematura defasagem do regime jurídico de tratamento de dados pessoais.

Seguindo-se à análise específica dos princípios, portanto, o princípio da finalidade está disposto no Art. 6º, inciso I, que assim normatiza: “finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (BRASIL, 2018).

Portanto, “[...] qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados” (DONEDA, 2015, p. 376). E, também sobre a temática, segundo Siqueira (2019, p. 31), para a devida observância ao princípio da finalidade:

> Deverá o controlador buscar sempre descrever, da forma mais pormenorizada e detalhada possível, de maneira destacada das demais cláusulas contratuais: (a) o propósito/finalidade do tratamento; (b) os meios empregados para a realização do tratamento; (c) a extensão e duração do tratamento, estabelecendo um marco temporal para o seu encerramento e eliminação dos dados; (d) informações de contato do controlador; e (d) informações acerca do uso compartilhado de dados pelo controlador.

Logo, o princípio da finalidade impõe que o tratamento dos dados pessoais deve observar o fim que espera o titular de dados, com base na relação estabelecida entre as partes e em tudo o quanto informado ao titular de dados, de modo que o agente de tratamento não pode desvirtuar o fim estabelecido inicialmente, operando tratamento para outra finalidade senão aquela informada ao titular de dados.

Em termos práticos, o princípio da finalidade permite restringir a transferência de dados pessoais a terceiros e serve de critério para analisar se é razoável ou não o tratamento dos dados para uma dada finalidade, de forma a possibilitar a indicação de abusividade no tratamento caso o tratamento viole essa finalidade (DONEDA, 2015, p. 376).

Em seguida, nos incisos II e III do Art. 6º, a LGPD prevê os princípios da adequação e da necessidade, respectivamente, os quais estão intrinsecamente ligados ao princípio da finalidade.

Assim, o Art. 6º, inciso II, dispõe: “adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”. Vainzof (2019, p. 142) argumenta que o princípio da adequação “[...] está vinculado ao da finalidade, pois prevê que o tratamento de dados pessoais somente pode ser realizado quando houver compatibilidade com as finalidades informadas ao titular, de acordo com o contexto do tratamento”.

A diferença, portanto, entre o princípio da adequação e da finalidade reside no fato de que “enquanto o último se preocupa com a regularidade da finalidade em si, o segundo aborda o procedimento realizado para chegar à finalidade pretendida” (COTS; OLIVEIRA, 2018, p. 101).

Portanto, o tratamento adequado dos dados pessoais, que observa esse princípio, deve respeitar, na execução do tratamento em si, a finalidade informada ao titular de dados que fundamenta o tratamento dos dados pessoais, estando proibido, dessa maneira, por ser inadequado, o tratamento dos dados por outros meios.

Seria o caso, por exemplo, de o agente de tratamento informar que compartilha os dados somente com uma empresa de gestão, mas compartilhá-lo com outras empresas, por exemplo, para efeitos de direcionar publicidade ao titular de dados.

Adiante, pelo princípio da necessidade, insculpido o Art. 6º, inciso III, normatiza a LGPD: “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" (BRASIL, 2018).

Explica Doneda (2015, p. 377) que pelo princípio da necessidade "[...] devem ser coletados e tratados somente os dados pessoais que são necessários para o atendimento de uma determinada finalidade, descartando-se os dados exorbitantes".

Siqueira (2019, p. 34) anota um exemplo que expressa a aplicação prática do princípio da necessidade, "[...] como quando um estabelecimento comercial solicita ao consumidor a identificação de seu tipo sanguíneo ou nome da mãe como condição para a comercialização de um produto".

Desta maneira, o princípio da necessidade impõe que ao agente somente é lícito tratar os dados pessoais que sejam necessários à finalidade apontada, de modo a minimizar o tratamento dos dados ao máximo, valendo-se tão somente daqueles dados cujo tratamento faça sentido de acordo com a atividade a ser desenvolvida e a finalidade informada ao titular de dados. Este princípio constitui a difundida ideia de minimização do tratamento de dados pessoais. Deve-se tratar o mínimo necessário à finalidade cientificada ao titular de dados.

Em seguida, o princípio do livre acesso está normatizado no inciso IV do Art. 6º da LGPD. O dispositivo assim estabelece: "livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (BRASIL, 2018).

Leciona Doneda (2015, p. 376-377) que pelo princípio do livre acesso "[...] o indivíduo tem acesso ao banco de dados onde suas informações estão armazenadas, podendo obter cópias destes registros, com a consequente possibilidade de controle destes dados".

E no mesmo sentido Vainzof (2019, p. 148) explica que do conteúdo do princípio do livre acesso, se depreende a possibilidade de o titular de dados "[...] constantemente acompanhar a utilização de seus dados pessoais junto ao controlador, de forma a controlar o fluxo informacional que lhe diga respeito, avaliar eventuais inexatidões para que possam ser corrigidas [...]".

Por consequência, é pelo princípio do livre acesso que "[...] os agentes de tratamento deverão disponibilizar procedimento que garanta ao titular a possibilidade de obter, a seu exclusivo critério, informações precisas acerca do tratamento de seus dados" (SIQUEIRA, 2019, p. 35).

Desse modo, pelo princípio do livre acesso, a agente de tratamento deverá disponibilizar meios para que o titular de dados consulte toda a cadeia de tratamento dos dados pessoais fornecidos, de modo que o titular de dados tenha direito a saber como é feito o tratamento, quanto tempo leva cada procedimento de tratamento, bem como quais de seus dados pessoais fornecidos são tratados em cada procedimento.

Já no Art. 6º, inciso V, reside o princípio da qualidade dos dados: “qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento”.

Para Doneda (2015, p. 376) o princípio da qualidade impera que “[...] os dados armazenados devem ser fieis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade”.

Considerável identificar alguns dentre os vários efeitos práticos que a imprecisão de dados pessoais pode ocasionar ao seu respectivo titular:

> Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta.
> Pior, uma vez coletado e tratado o dado pessoal impreciso, sem que seja sanada a respectiva imprecisão na fonte, o risco de que esse dado viciado seja tratado de forma permanentemente incorreta é bastante elevado (VAINZOF, 2019, p. 149).

Então, pode-se anotar que o princípio da qualidade de dados impõe ao agente de tratamento que zele para que os dados pessoais objeto de seu tratamento espelhem a realidade dos dados pessoais do respectivo titular, adotando medidas para que não haja equívocos durante o tratamento desde a coleta até a sua eliminação/exclusão, e, ainda, para que se mantenham atualizados os dados, de modo a obrigar o agente de tratamento, também, a manter práticas que visem afastar, periodicamente, eventual defasagem dos dados pessoais.

Segue-se a abordagem dos princípios, a indicar-se, agora, o da transparência, na forma do Art. 6º, inciso VI, da LGPD: “transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial” (BRASIL, 2018).

Enfatiza Vainzof (2019, p. 150), que “[o] titular de dados carece da ampla informação sobre o tratamento dos seus dados para que consiga enxergar, cristalinamente, a legalidade, a legitimidade e a segurança do tratamento de acordo com o seu propósito, adequação e necessidade”.

Quer dizer, portanto, que para que o titular de dados possa verificar a observância da LGPD e da legalidade em geral do tratamento de seus dados junto a determinado agente de tratamento, é preciso que tenha informações muito claras sobre a forma como o tratamento é realizado e quem são os agentes de tratamento dos seus dados.

Aqui, importante ressaltar que o dispositivo ressalva os segredos comercial e industrial, e com razão. A um controlador, por exemplo, não é exigido que abra toda a sua lista de fornecedores, expondo, assim, toda a sua cadeia de parceiros comerciais que fazem parte da estrutura intrínseca de sua atividade empresária.

Todavia, pelo princípio da transparência, deve esse controlador, por exemplo, dar transparência sobre quantos agentes de tratamento fazem parte da cadeia de tratamento dos dados pessoais e explicar, de maneira geral, o tratamento de dados realizado por cada agente, sem que seja necessário abrir, assim, o nome de parceiros comerciais ou dar detalhes das operações comerciais.

É o caso, por exemplo, de um serviço de *streaming* que informa que as transações realizadas por meio de cartão de crédito contam com agentes de tratamento que fazem a intermediação do pagamento e que fazem a análise antifraude da transação. Veja-se: não é necessário apontar quem são esses parceiros comerciais ou abrir as cláusulas dos contratos mantidos com esses agentes de tratamento, ou dar detalhes como os valores desses contratos empresariais.

Portanto, o princípio da transparência pretende permitir ao titular de dados entender toda a cadeia de tratamento de seus dados pessoais, estando tal princípio limitado à não violação de segredos industriais e comerciais.

Por sua vez, o princípio da segurança está no inciso VII do Art. 6º: “segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (BRASIL, 2018).

Quer dizer, assim, que “[o]s agentes devem adotar todas as medidas razoáveis e que estejam ao seu alcance para prevenir que os dados sejam alvos de vazamento e acesso não autorizado” (SIQUEIRA, 2019, p. 39).

Doneda (2015, p. 377) trata do “princípio da segurança física e lógica”, segundo o qual “os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado”.

Relevante apontar que as medidas que devem ser adotadas pelo agente de tratamento são medidas razoáveis. Não se exige a adoção de posturas extravagantes, mas aquelas que sejam objetivamente razoáveis para a proteção dos dados pessoais dentro de um certo contexto e de acordo com o desenvolvimento tecnológico da época.

Interessa indicar, aqui, que a ANPD poderá estabelecer regramento específico para estabelecer o que são essas medidas técnicas e administrativas para dar alguma concretude sobre o princípio da segurança, conforme dispõe o Art. 46, § 1º da LGPD (BRASIL, 2018).

Dessarte, os agentes de tratamento devem empregar todos os meios de segurança a fim de proteger os dados pessoais, tanto medidas físicas quanto medidas eletrônicas, a fim de mantê-los indenes, impedindo, assim, que sejam acessados, modificados, excluídos/destruídos, transmitidos, etc.

Explicitado no Art. 6º, inciso VIII, o princípio da prevenção tem o seguinte conteúdo: “[...] prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais” (BRASIL, 2018). O princípio da prevenção relaciona-se também com o princípio da segurança e também com as boas práticas, mas por “prevenção” quer significar que os agentes de tratamento devem adotar medidas que impeçam incidentes de dados, ou seja, não basta que os agentes de tratamento tenham planos de ação muito bem elaborados para casos de vazamentos de dados e nem que tenham provisionados valores para indenizar satisfatoriamente os titulares de dados em um caso como este, por exemplo, mas devem adotar medidas que tenham por objetivo evitar, ao máximo, a ocorrência de incidentes de quaisquer categorias.

Para concluir, notórias as ponderações de Vainzof (2019, p. 158) sobre as boas práticas relacionadas à proteção de dados pessoais:

> A LGPD é uma norma que visa modificar a cultura no tratamento de dados pessoais para que riscos sejam mitigados desde antes do tratamento, evitando-se ao máximo qualquer hipótese, sempre presente, de violação de dados pessoais. No decorrer da Lei há uma motivação nítida nesse sentido, impondo que os agentes de tratamento, desde a concepção da iniciativa que visa tratar dados pessoais e durante todo o seu ciclo de vida, que termina com o seu

> descarte, reflitam, analisem e adotem medidas efetivas para garantir a legalidade dos procedimentos e a proteção desse insumo tão valioso, mas ao mesmo tempo, tão perigoso, se tratado de forma irregular.

No mesmo sentido, Siqueira (2019, p. 40-41) explica a necessidade de serem observadas pelo agente de tratamento "[...] as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos [...]".

Logo, pelo princípio da prevenção deve-se promover a adoção de medidas para evitar todo e qualquer incidente de dados pessoais, visando-se, portanto, a reorganização de procedimentos internos da atividade do agente de tratamento, com o objetivo de evitar, ao máximo, a ocorrência de incidentes de dados, inclusive, dentre outros, por meio de ações educativas direcionadas a todos os sujeitos que se envolvam de qualquer forma com tratamentos de dados pessoais. Ressalta-se que as previsões específicas sobre segurança e boas práticas estão dispostas no Art. 46 da LGPD, as quais serão objeto de estudo específico na seção apartada, à frente.

A não discriminação nas atividades de tratamento de dados é também um princípio disposto na LGPD, no Art. 6º, inciso IX, que determina, literalmente: "não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018).

Vainzof (2019, p. 161-162) explica que o princípio da não discriminação se pode depreender da própria diferenciação entre privacidade e proteção de dados, haja vista que esta vai além daquela, de modo que o princípio da não discriminação pretende afastar possibilidades de estigmatização do ser humano, bem como proibir o tratamento dos dados pessoais para criação de estereótipos (classificação) ou para limitar direitos (segregação).

É de se lembrar o conteúdo do direito à proteção de dados pessoais, nesse sentido, cujo fim estabelece o livre desenvolvimento da personalidade, sem ingerências externas embasadas no tratamento de seus dados pessoais.

Assim, são exemplos de violação ao princípio da não discriminação: "(i) realizar senso para dispensa de empregados de determinada religião; (ii) deixar de descrever a abrangência do tratamento realizado; (iii) não fornecer fácil acesso às informações de tratamento" (COTS; OLIVEIRA, 2018, p. 102).

Como último princípio elencado no Art. 6º da LGPD, o inciso X normatiza a responsabilização e prestação de contas, nos seguintes termos: “responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (BRASIL, 2018).

> Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo o ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos (VAINZOF, 2019, p. 166-167).

Ou seja, a LGPD deixa claro que os agentes de tratamento devem adotar todas as medidas de segurança necessárias, devem posicionar boas práticas em suas atividades, sob pena de serem responsabilizados.

Além das responsabilidades nas demais esferas do Direito, a prática de ilícitos no tratamento de dados pessoais responsabiliza o agente de tratamento de maneira administrativa de forma a sujeita-lo às sanções previstas no Art. 52. O princípio da responsabilização e prestação de contas, porém, não significa a mera responsabilização e adoção de medidas adequadas no tratamento de dados pessoais.

Observe-se que a LGPD previu expressamente a “demonstração” pelo agente de tratamento quanto à adoção dessas medidas para cumprimento das normas de proteção de dados e da eficácia dessas medidas. E isso significa que o princípio determina que os agentes de tratamento provem a adoção e a respectiva eficácia dessas medidas, de modo que devem demonstrar por meio de relatórios, pautas, declarações, registros em plataformas e softwares, as medidas praticadas para observar a LGPD e a respectiva eficácia dessas medidas. O ideal aqui, portanto, é que o agente de tratamento documente todas essas medidas, de maneira a facilitar, assim, essa comprovação exigida expressamente no inciso X.

Dessa forma, na aplicação da LGPD se faz essencial a observância de todos os princípios insculpidos no Art. 6º, por constituírem normas que devem nortear toda a atividade de tratamento de dados pessoais e, inclusive servem como critério interpretativo tanto de outros princípios quanto de regras da LGPD. E, por isso, o DPO,

no exercício de suas atividades, deve-se pautar por referidos princípios, na máxima medida possível, conjugando-os com as demais normas do sistema jurídico brasileiro e previstas na própria LGPD.

3.3 Direitos dos titulares

Os direitos dos titulares de dados estão dispostos do Arts. 17 ao 22 da LGPD, sendo o Art. 19 a esquematização prática para o exercício desses direitos. São os Arts. contidos no Capítulo III da LGPD. Como já retro mencionado, as regras estabelecidas como direitos dos titulares de dados servem para dar concretude ao fundamento da autodeterminação informativa, para instrumentalizar o poder de o titular de dados decidir, naquilo que for cabível, os limites do tratamento de seus dados pessoais.

Mas não somente isso. Os direitos dos titulares de dados, como se verá, dão concretude aos princípios dispostos no Art. 6º da LGPD, sendo muito clara, na maioria dos direitos estabelecidos, a relação intrínseca com as normas principiológicas de proteção de dados pessoais e com o fundamento da autodeterminação informativa. Ou seja, o Art. 6º dispõe os princípios e o Capítulo III arrola os direitos dos titulares decorrentes dessas normas.

Assim, o Art. 17 reforça que a pessoa natural é titular de seus dados e reitera as garantias de liberdade, intimidade e privacidade: “[t]oda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei” (BRASIL, 2018).

O Art. 18 elenca um rol, não taxativo, de direitos do titular de dados e em seus respectivos parágrafos rege, de maneira mais concreta, a forma de realizar tais direitos. O Art. 19 segue o mesmo objetivo dos parágrafos do artigo anterior. Após, os Arts. 20, 21 e 22 tecem direitos diversos e autônomos daqueles elencados no Art. 18, não se tratando de extensão ou instrumentalização dos listados no rol do Art. 18.

É obrigatório explicar que os direitos dos titulares de dados não se limitam aos que constam no Capítulo III da LGPD, e que podem ser depreendidos demais direitos esparsos ao longo da Lei.

A compreensão dos direitos dos titulares de dados se faz essencial, como se verá à atuação do DPO. Responsável por intermediar a relação entre o agente de tratamento e os titulares de dados, este deve atuar de modo a realizar os direitos dos

titulares, respondendo-os, diretamente, inclusive. Por essa razão, dado o escopo do presente trabalho, se faz essencial a abordagem dos direitos dos titulares de dados.

Nessa toada, o Art. 18 da LGPD determina em seu *caput*: “[o] titular de dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...]”. E, doravante, lista os direitos específicos em seus respectivos incisos, do I ao IX, com as especificações dos §§ 1º ao 8º.

O primeiro direito é a “confirmação da existência de tratamento” (BRASIL, 2018), do inciso I do Art. 18. O direito de confirmar a existência do tratamento se relaciona, assim, com os princípios do livre acesso, da qualidade dos dados e da transparência, conforme Art. 6º, incisos IV, V e VI da LGPD.

Por tal direito, o titular de dados pode confirmar a existência do tratamento sem que precise apresentar qualquer justificativa ao controlador, a poder-se depreender, ainda, do Art. 9º da LGPD, que o titular de dados deve ser informado sobre o início do tratamento dos dados ainda que não solicite tal informação, ou seja, o titular de dados deve ter conhecimento sobre o tratamento tão logo operada a coleta dos dados (MALDONADO, 2019, p. 221-222). Assim, o titular de dados tem o direito de saber se o controlador promove o tratamento de seus dados pessoais desde que lhe coletados os dados pessoais.

Complementa o direito à confirmação da existência o direito de “acesso aos dados”, na forma do inciso II do Art. 18 (BRASIL, 2018), também atrelado aos princípios do livre acesso, da qualidade dos dados e da transparência, conforme Art. 6º, incisos IV, V e VI da LGPD.

Antes de o titular de dados exercer o direito de acesso, é pressuposto a existência do tratamento, após o qual, portanto, o primeiro poderá ser exercido, a possibilitar, assim, que o titular de dados acesse diversas informações: “[...] finalidades, categorias, destinatários, prazo de conservação, origem dos dados, existência de decisões automatizadas, apenas para elencar algumas” (MALDONADO, 2019, p. 222). Desse modo, o direito de acesso caracteriza-se pelo poder conferido ao sujeito de entender todas as atividades que envolvem o tratamento de seus dados de forma ampla.

Em referência tanto ao direito de confirmação da existência do tratamento quanto do direito de acesso, o Art. 19 da LGPD dispõe sobre a forma por meio da qual tais direitos podem ser exercidos, a garantir, assim, que após a requisição do titular,

o controlador deverá responder de forma simplificada e imediatamente caso se trate de uma requisição simples ou no prazo de quinze dias a partir do requerimento em situações de tratamento de maior complexidade (BRASIL, 2018). Ainda no Art. 19, seu § 1º determina o armazenamento em meio que facilite o exercício do direito de acesso enquanto o § 2º dá a faculdade ao titular de dados de solicitar os dados por meio eletrônico ou impresso (BRASIL 2018). Por fim, o § 3º permite a solicitação de cópia integral dos dados pessoais quando o tratamento for fundamentado em consentimento ou em contrato em formato que admite utilização posterior, inclusive em outras operações de tratamento (BRASIL, 2018).

O “direito de correção de dados incompletos, inexatos ou desatualizados” está elencado no inciso III do Art. 18. Assim, “[...] os dados devem ser atualizados por decorrência de alteração de nome, endereço, estado civil, gênero, entre outros, desde que, por óbvio, haja a devida e formal requisição do titular ao controlador” (MALDONADO, 2019, p. 224).

É denominado, comumente, por direito de retificação, e está intimamente ligado ao princípio da qualidade dos dados, conforme Art. 6º, inciso V, da LGPD, de forma que autoriza ao titular de dados a correção de seus dados pessoais junto ao controlador, em qualquer tempo, o que torna importante consignar que “[...] a falta de acurácia dos dados é elemento que potencialmente pode viabilizar fraudes, notadamente em ambiente on-line” (MALDONADO, 2019, p. 224).

Dessa forma, o direito de corrigir os dados incompletos, inexatos ou desatualizados, guarda relação com o princípio da qualidade de dados, pode ser exercido pelo titular de dados em qualquer tempo, porém, não obriga ao controlador que tenha ciência de atualizações das informações pessoais, e se põe como direito essencial para o fim de evitar a prática de fraudes.

No inciso IV do Art. 18 estão previstos, conjuntamente, os direitos de “anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei”. Frisa-se que os conceitos de dado anonimizado, de bloqueio e eliminação estão dispostos no Art. 5º da LGPD, a dispensar demais comentários a respeito.

Cots e Oliveira (2018, p. 159), ponderando sobre os direitos de confirmação da existência do tratamento, acesso e retificação dos dados e anonimização, bloqueio ou eliminação dos dados, indicam a inter-relação entre eles: “[o] titular tem direito a ter a confirmação da existência de tratamento, acesso aos dados tratados e a corrigir,

quando incompletos, inexatos ou desatualizados” ao que se segue a possibilidade de solicitar a anonimização, bloqueio ou eliminação dos dados:

> Se for constatado pelo titular que há dados necessários ou excessivos, bem como, se o tratamento estiver se dando em desconformidade com a finalidade prevista, o titular poderá exigir a anonimização, bloqueio ou eliminação de dados. O titular poderá especificar qual dessas ações deverá ser tomada (anonimização, bloqueio ou eliminação)? A nosso ver o titular não possui conhecimento técnico para tomar essa decisão, cabendo ao controlador adotar a medida que afaste a incidência da LGPD, mas, por outro lado, que atenda aos seus interesses (por exemplo, a anonimização pode ser mais benéfica do que a eliminação, se houver interesse em dados estatísticos) (COTS; OLIVEIRA, 2018, p. 159).

Esses direitos claramente são uma expressão concreta do princípio da necessidade ou minimização do tratamento de dados, ou seja, possibilitam ao titular de dados que pleiteie a anonimização, bloqueio ou eliminação a fim de retirar da atividade de tratamento todo e qualquer dado além daquele mínimo que faça cumprir a finalidade do tratamento.

O direito de “portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial” se insere no inciso V do Art. 18 da LGPD (BRASIL, 2018). Tal direito não é exigível caso já tenha ocorrido o procedimento de anonimização desses dados, conforme o § 7º do Art. 18 (BRASIL, 2018). Logo, “Com a obrigatoriedade de atendimento ao direito de portabilidade, permite-se ao titular dos dados encaminhá-los a outro controlador de maneira fácil e estruturada” (MALDONADO, 2019, p. 232).

Cots e Oliveira (2018, p. 160) explicam, porém, que os dados pessoais em si não se confundem com o produto da atividade de tratamento, o que significa dizer que caso um agente de tratamento tenha, por exemplo, criado um perfil com base na navegação de um usuário logado utilizando-se de técnicas e estudos para tanto, este agente não é obrigado a transferir o perfil criado, mas tão somente os dados da navegação em si.

Via de consequência, o que a LGPD garante ao titular é a transferência dos dados ao agente que indicar, sem que se transfira o produto da atividade de tratamento operada pelo agente anterior.

Adiante, no inciso VI do Art. 18, a LGPD prevê o direito de “eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses

previstas no art. 16 desta Lei". Sobre referido direito, Maldonado (2019, p. 222) comenta: "[p]or evidente, quem fornece o consentimento pode igualmente retirá-lo quando assim lhe aprouver".

Referido direito se relaciona às bases legais de tratamento referentes ao consentimento, seja para dados simples ou dados sensíveis, como se explicará a seguir. O fato é que conferido o consentimento pelo titular de dados, este poderá revoga-lo. Esta é das demonstrações mais concretas da autodeterminação informativa. O titular de dados pode decidir quanto ao tratamento, de modo que pode consentir e, a seu critério, revogar o consentimento.

A ressalva relativa ao Art. 16 se cinge à circunstância de que, em certas hipóteses, o agente de tratamento deve conservar os dados, hipóteses estas que estão elencadas no referido dispositivo, quais sejam, para cumprir obrigação normativa, para estudo por órgão de pesquisa, para transferência a terceiro ou para uso exclusivo do controlador (BRASIL, 2018).

Sublinhe-se, ainda, que os §§ 3º e 4º do Art. 18 da LGPD preveem que o titular de dados pode exercer os seus direitos por meio de simples requerimento ao que o controlador deverá responder, a poder comunicar que não é o agente de tratamento, indicando, neste caso, o agente, caso saiba, ou ainda poderá indicar quais razões, de fato ou de direito, o impedem de adotar a medida pleiteada pelo titular.

O direito de pleitear a eliminação previsto no inciso VI é específico quanto ao tratamento fundamentado na base legal do consentimento, o que se justifica pela peculiaridade que essa base legal assume, de modo a garantir ao titular de dados que da mesma maneira que consentiu com o tratamento, poderá, na outra mão, pleitear a eliminação dos dados.

Por fim, destaca-se que essa eliminação não demanda juízo de inadequação ou desnecessidade do tratamento dos dados, sendo direito do titular pleiteá-la sem que aponte esses fundamentos para tanto ou quaisquer outros, cuja exigência, se operada pelo controlador, será considerada ilícita.

O Art. 18, no inciso VI, dispõe sobre o direito à "informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados" (BRASIL, 2018). Referido direito está em consonância, claramente, com os princípios do livre acesso e da transparência, dispostos no Art. 6º, incisos IV e VI.

Dessa forma, "[u]ma vez que é permitido tal uso compartilhado nos termos da lei, assegura-se ao titular dos dados pessoais buscar informação acerca das

entidades públicas e privadas com as quais o controlador realizou o uso compartilhado" (MALDONADO, 2019, p. 233).

Assim, o titular de dados poderá solicitar informações sobre os compartilhamentos realizados pelo controlador, sejam eles relacionados a órgãos públicos ou privados, tudo com vistas a dar a maior transparência e acesso possível sobre toda a cadeia da atividade de tratamento operada.

A "informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa" é o direito disposto no inciso VII do Art. 18 da LGPD. Também está atrelado ao princípio da transparência, na forma do Art. 6º, inciso VI, da LGPD.

O que o dispositivo prevê é o direito de o titular solicitar essa informação e, assim, ser respondido pelo controlador sobre a possibilidade de não consentir e quais serão os efeitos da ausência do seu consentimento. Entretanto a postura que deve ser adotada pelo controlador, com base nos deveres de transparência e de informação, é antecipar-se e informar, com clareza, se o titular de dados poderá deixar de consentir ou não e o que decorrerá desse não consentimento (MALDONADO, 2019, p. 234).

Assim, do próprio espírito da LGPD e de suas bases principiológicas, o titular de dados, antes mesmo do início do tratamento, deve ter ciência e informação clara sobre se pode ou não consentir e as consequências disso, porém, na hipótese em que isso não ocorra, por prescrição explícita do inciso VII do Art. 18, o controlador fica obrigado a informa-lo mediante requisição realizada pelo titular de dados.

Como último direito elencado no rol do Art. 18, o inciso IX dispõe: "revogação do consentimento, nos termos do § 5º do art. 8º desta Lei" (BRASIL, 2018). Trata-se, aqui, da possibilidade de o titular de dados revogar o consentimento de modo a impedir, imediatamente, toda e qualquer atividade de tratamento cuja base legal se restrinja ao consentimento. Conforme dispõe o Art. 8º, § 5º da LGPD: "consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado [...]" (BRASIL, 2018).

O consentimento, portanto, como lhe é próprio, pode ser revogado a qualquer tempo. Não à toa a LGPD se ocupa de forma pormenorizada e em diversas passagens, de assegurar a mais plena autodeterminação informativa mormente quando se trata da base legal de tratamento do consentimento.

E para revogar o consentimento o titular de dados não necessita demonstrar qualquer ilicitude no tratamento de seus dados, bastando, simples e injustificadamente, que manifeste a revogação, ao que, ato contínuo, deve seguir a imediata cessação de qualquer forma de tratamento dos dados, salvo se houver alguma outra base legal que autorize prosseguir o tratamento.

Como será mais bem visto a seguir, para o tratamento de dados é preciso que o agente esteja autorizado por uma das hipóteses previstas nos Arts. 7º e 11 da LGPD, sendo uma delas o consentimento. E, desse modo, se o controlador possui apenas autorização para tratar os dados devido ao consentimento que o titular de dados lhe conferiu, em qualquer tempo que revogue o consentimento, deverá cessar a atividade de tratamento. Se autorizado sob outra hipótese, poderá prosseguir o tratamento, na exata medida do que aquela base legal o autoriza.

Cumpre consignar, por fim, que "[...] a revogação do consentimento não produz quaisquer efeitos no que se refere aos atos praticados sob a égide do consentimento licitamente fornecido, ratificando-se, portanto, o tratamento anteriormente realizado" (MALDONADO, 2019, p. 235).

Nesse sentido, o titular de dados tem o direito de revogar, em qualquer tempo, o seu consentimento quanto ao tratamento de dados, do que deve ocorrer a imediata cessação do tratamento pelos agentes, salvo se houver outra base legal que o autoriza, mantendo-se indenes as atividades de tratamento praticadas com base no consentimento anteriormente conferido.

Assim, veja-se que os direitos dos titulares de dados elencados no Art. 18 em muitos pontos se inter-relacionam, e, por vezes, podem em situações práticas até mesmo vir a causar confusão quanto categorizar devidamente qual direito está sendo exercido. É certo que o regular delineamento dos direitos se torna imprescindível por haver disposições específicas para lhes dar efetividade. Todavia, ao que aparenta, pretendeu o legislador pecar pelo excesso a deixar faltar previsão normativa e, assim, correr o risco de deixar desprotegido sob algum aspecto o titular de dados.

Além desses direitos, que objetivam explicitamente concretizar em favor dos titulares de dados os princípios da proteção de dados pessoais, é importante apontar outros três direitos que se pode extrair dos Arts. 20, 21 e 22 da LGPD.

O Art. 20, assim, estabelece o direito à revisão e à explicação sobre decisões tomadas de forma automatizada:

> O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (BRASIL, 2018).

Referido artigo cuida especialmente de indicar o que se entende por *profiling*, ou seja, quando o tratamento dos dados cria um perfil para o titular de dados e o incluem em uma determinada categoria que poderá lhe definir um destino, por exemplo, a recusa de concessão de crédito tomada de forma automatizada com base em um perfil de consumo do titular de dados.

O direito à não lesão pelo exercício regular de direitos está disposto no Art. 21 da LGPD, que dispõe: “[o]s dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo” (BRASIL, 2018). Pelas práticas que se observa no mercado, o objetivo é proibir que os agentes de tratamento se utilizem dos dados pessoais do titular para lesá-lo, por exemplo, na situação em que venha a propor demanda judicial em face de uma instituição bancária.

Em um contexto como esse, não poderá se valer a instituição bancária para lesar ou anotar potencial prejuízo ao titular de dados tão somente porque, neste exemplo, exerce seu direito de ação.

E, por fim, o Art. 22 dispõe sobre a possibilidade de o titular de dados ter os seus direitos tutelados por meio de demanda individual ou coletiva: “A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva” (BRASIL, 2018).

Interessante demonstrar que referida previsão está em consonância com o que dispõe o Art. 81 do CDC, segundo o qual “[a] defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo” (BRASIL, 1990).

Assim, a LGPD pretendeu munir o titular de dados de todas as formas para dar efetividade a todo o novo regramento de proteção dos dados pessoais. Nesse

sentido, “[...] considerando que o titular de dados é a figura central no sistema normativo, buscou assegurar ampla proteção, disponibilizando a ele inúmeras garantias no que se refere ao exercício de seus direitos” (MALDONADO, 2019, p. 243).

Logo, observa-se que diversos são os direitos conferidos aos titulares de dados, não se limitando, reitera-se, às previsões do Capítulo III. Considere-se, ainda, que a principiologia da proteção de dados pessoais, como é de sua própria posição nessa categoria de norma, orienta toda e qualquer atividade de tratamento, por qualquer agente que seja, de forma que dos princípios pode-se extrair, na análise dos casos concretos, incontáveis situações que garantam direitos aos titulares de dados.

Ao DPO, por sua vez, caberá, sobretudo, compreender os fundamentos e a principiologia da proteção de dados pessoais, de maneira a ter aptidão para ponderar que, além dos direitos expressamente previstos na LGPD, se poderão extrair incontáveis conclusões que caracterizem direitos aos titulares de dados quando posta a situação concreta à análise de todo o regime jurídico, mormente, os princípios estabelecidos na LGPD.

3.4 Bases legais de tratamento

As bases legais de tratamento são as hipóteses em que a LGPD permite o tratamento de dados pessoais. Isso quer dizer que a LGPD institui uma nova sistemática quanto à legalidade do tratamento de dados, no sentido de que, se antes o tratamento de dados poderia ocorrer em qualquer hipótese, agora poderá ocorrer somente das hipóteses listadas na própria LGPD. Ou seja, para ser lícito o tratamento de dados, em primeiro lugar, deve-se analisar se ele está autorizado em ao menos uma das bases legais.

Anota-se que não se objetiva adentrar no alcance das bases legais de tratamento, nem se enveredar nas nevrálgicas problemáticas respeitantes às bases legais do consentimento e do legítimo interesse. Pretende-se, nesta seção, conferir uma compreensão sobre o manejo das bases legais do ponto de vista macro, afastando-se do escopo a discussão do conteúdo de cada uma.

Desse modo, a LGPD trouxe uma sistemática que divide as bases legais de tratamento, primeiro, pela categoria dos dados. Dessa forma, para o tratamento de dados pessoais simples as bases legais são as do Art. 7º. De outro lado, para o tratamento de dados pessoais sensíveis deve-se observar as bases legais do Art. 11.

Comenta Wimmer (2019, p. 131):

> Como se depreende da leitura do *caput* dos arts. 7º e 11, a lei buscou reunir nesses dois dispositivos a totalidade das bases legais para o tratamento de dados pessoais: não por acaso, ambos os artigos declaram que o tratamento **somente** será possível nas hipóteses ali delineadas.

A LGPD buscou, dessa forma, elencar as hipóteses taxativas em que se admite o tratamento de dados pessoais, de forma que a legalidade do tratamento fica submetida a enquadrar-se a situação fática, se de dados pessoais simples, a uma das hipóteses do Art. 7º, se de dados pessoais sensíveis, a uma das hipóteses do Art. 11.

Faz-se um adendo, aqui, para efeitos metodológicos, que quando se menciona neste trabalho “dados pessoais simples”, se faz para diferencia-los dos “dados pessoais sensíveis”, de modo que os dados pessoais simples significam, apenas, aqueles dados pessoais que não são sensíveis.

Os dados pessoais sensíveis são assim diferenciados porque as categorias de dados que assim são classificadas pela LGPD constituem circunstâncias que visam promover de modo muito mais incisivo a não discriminação do titular de dados. Como pontua Vainzof (2019, p. 91-92):

> Os dados pessoais sensíveis, em linhas gerais, são dados pessoais que possam trazer algum tipo de discriminação quando do seu tratamento (origem racial, convicção religiosa, opinião política, dado referente à saúde, para citar alguns exemplos) bem como, diante da sua criticidade, dados genéticos e biométricos. Ou seja, são dados pessoais que poderão implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares.
> A motivação da conceituação dessa categoria especial de dados pessoais é fruto de uma observação pragmática da diferença que apresenta o efeito do tratamento desses dados em relação aos demais.

Portanto, distinguem-se os dados pessoais simples dos dados pessoais sensíveis devido ao maior potencial destes em atentar contra as liberdades e garantias fundamentais do titular de dados, tendo em vista o maior potencial de impingir discriminação frente ao seu titular de dados. Daí que, por essa razão é que são diferenciados e, por serem diferenciados, os dados pessoais sensíveis se sujeitam a um regime jurídico diferenciado na LGPD.

Vainzof (2019, p. 92), explica, portanto, as diferenças a que se sujeita o tratamento de dados pessoais sensíveis conforme as disposições da LGPD:

> As bases legais para o tratamento de dados pessoais sensíveis são diferenciadas e limitadas, dispostas no art. 11, da LGPD;
> Quando a base legal para o tratamento for o consentimento, além de ser livre, inequívoco e informado, também deverá ser específico e destacado;
> Não há base legal para o tratamento de dados sensíveis por interesse legítimo;
> Não há base legal para o tratamento de dados sensíveis para a proteção do crédito. Inclusive, a Lei do Cadastro Positivo veda, expressamente, anotações de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e ética, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas";
> Da mesma forma, não há base legal para tratamento de dado sensível para a execução de contrato ou procedimentos preliminares relacionados a contrato, mas sim para o exercício regular de direitos, inclusive em contrato;
> Há base legal específica quando o tratamento de dado sensível servir para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos;
> A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores, com o objetivo de obter vantagem econômica, poderá ser objeto de vedação ou de regulamentação por parte da ANPD, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências;
> É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, exceto nas hipóteses de portabilidade de dados quando consentido pelo titular ou necessidade de comunicação para a adequada prestação de serviços de saúde suplementar.

Assim, os dados pessoais sensíveis são assim classificados para que se diferenciem dos dados pessoais simples devido ao maior potencial de afrontar contra as liberdades e garantias fundamentais do titular de dados, e, com base na distinção semântica, se sujeitam a um regime jurídico diferenciado na LGPD.

Para esclarecer a identidade e as diferenças entre as bases legais de tratamento de dados pessoais simples e sensíveis, apresenta-se a tabela a seguir, na qual também se atribui um resumo das bases legais a fim de facilitar a menção a estas e possibilitar, nesse sentido, identificar sobre o que se está a mencionar (BRASIL, 2018):

Base legal resumida	Dados pessoais simples (Art. 7º)	Dados pessoais sensíveis (Art. 11)
Consentimento	mediante o fornecimento de consentimento pelo titular, que deve ser livre, inequívoco e informado	quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas, além

		de também dever ser livre inequívoco e informado
Obrigação normativa	para o cumprimento de obrigação legal ou regulatória pelo controlador	cumprimento de obrigação legal ou regulatória pelo controlador;
Políticas públicas	pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei	tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos
Estudo por órgão de pesquisa	para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais	realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis
Execução de contrato	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	
Exercício regular de direito	para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)	exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)
Proteção da vida	para a proteção da vida ou da incolumidade física do titular ou de terceiro	proteção da vida ou da incolumidade física do titular ou de terceiro
Tutela da saúde	para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária	tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
Legítimo interesse	quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais	
Proteção ao crédito	para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente	
Prevenção à fraude		garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem

		direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Observa-se, portanto, que o Art. 7º traz o total de dez bases legais que autorizam o tratamento de dados, enquanto o Art. 11 prevê oito bases legais, sendo que há identidade entre sete das bases legais de tratamento: consentimento; obrigação normativa; políticas públicas; estudo por órgão de pesquisa; exercício regular de direito; proteção da vida; tutela da saúde. Ou seja, é possível o tratamento de dados pessoais simples e sensíveis, igualmente, em todas essas sete hipóteses.

E verifica-se, nesse sentido, que o Art. 7º autoriza o tratamento de dados pessoais simples nas situações de execução de contrato, legítimo interesse e proteção ao crédito, situações em que o tratamento de dados pessoais sensíveis não é admitido. De outro lado, para tratamento de dados sensíveis há a base legal de prevenção à fraude, que não aparece no rol do tratamento de dados pessoais simples.

Conforme apontado acima, são taxativos os róis dos dados pessoais simples e sensíveis, entretanto o que se exige é o enquadramento em ao menos uma das hipóteses, sendo possível que para uma mesma atividade de tratamento haja mais de uma base legal que o autorize. Nesse sentido, “[o] tratamento pode se dar mediante mais de uma base legal, como poderia ser o caso, por exemplo, do consentimento aliado à necessidade de cumprimento de obrigação legal” (COTS; OLIVEIRA, 2018, p. 104).

Verifica-se aqui simples raciocínio a partir do princípio geral de Direito segundo o qual a prerrogativa menor é autorizada pela prerrogativa maior: se é lícita a atividade de tratamento fundada em uma base legal, com muito mais razão pode-se realizar o tratamento de dados fundado em duas ou mais bases legais. Quem pode o mais (tratar dados sob uma só base legal), pode o menos (tratar dados em mais de uma base legal).

Daqui já se pode concluir que para ser lícito o tratamento dos dados, deve-se observar uma das hipóteses taxativas do Art. 7º, para os dados pessoais simples, e ao menos uma das hipóteses taxativas do Art. 11, para os dados pessoais sensíveis, e que o tratamento deve se enquadrar em ao menos uma das bases legais, a ser possível que haja respaldo em mais de uma delas.

Soma-se a isso o fato de que é possível haver o tratamento de apenas dados pessoais simples, porém, sempre que houver tratamento de dados pessoais sensíveis

haverá o tratamento de dados pessoais simples. Não é possível, por exemplo, tratar a prescrição de um medicamento como um dado pessoal sensível sem que haja o tratamento do dado pessoal simples, por exemplo, o nome do paciente que solicitou atendimento médico e a quem foi direcionada a prescrição de medicamento.

A despeito de se ter afastado deste trabalho a análise dos conceitos previstos na LGPD, aqui é relevante pontuar, para este raciocínio, que os dados pessoais sensíveis são aqueles referentes a “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” (BRASIL, 2018).

Enfatiza-se, portanto, que não há como se caracterizar um dado pessoal, por exemplo, de origem racial (dado sensível) se a ele não estiver atrelado, ao menos, um nome (dado simples). Ou seja, “caucasiano” não é um dado pessoal, mas atrelado, ao menos, a um nome, ou a um RG, ou CPF, enfim, torna-se um dado pessoal sensível e, junto a ele, haverá sempre, ao menos, um dado pessoal simples, de forma que em qualquer atividade de tratamento de dado sensível deve-se encontrar a base legal que o autoriza e, em conjunto, a base legal que autorize o tratamento do dado pessoal simples.

Assim, para todo tratamento de dado pessoal sensível haverá tratamento de dado pessoal simples. Do contrário, eventual informação 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” (BRASIL, 2018) nem sequer será considerada um dado pessoal.

Logo, nota-se ser necessário, para o tratamento dos dados pessoais, realizar o enquadramento da atividade em uma das hipóteses dos Arts. 7º e 11, sendo possível enquadrar a atividade em mais de uma das bases legais e, ainda, necessário, sempre que houver dados sensíveis, enquadrar os demais dados em uma das bases legais de tratamento de dados simples. Essa é a separação por categoria de dados que a LGPD dispõe.

Ainda, há uma divisão das bases legais de tratamento dos Arts. 7º e 11, que a despeito de não definida na LGPD, é sensível para o jurista que as analisa. Nessa toada, é possível separar as hipóteses de tratamento em “finalísticas” e “não finalísticas”.

As hipóteses de tratamento finalísticas são aquelas que já estão ligadas com a finalidade do tratamento dos dados, de forma que designam, por si só, ainda que de maneira geral, para que será realizado o tratamento dos dados pessoais. São bases legais finalísticas: obrigação normativa; políticas públicas; estudo por órgão de pesquisa; execução de contrato; exercício regular de direito; proteção da vida; tutela da saúde; proteção ao crédito; prevenção à fraude.

Quer dizer, quando a base legal, por exemplo, é “execução de contrato”, já se pode depreender que os dados serão tratados para cumprimento das obrigações contratuais. Se os dados são tratados sob a base legal da tutela da saúde, já se sabe que a finalidade está relacionada a uma atividade médica em benefício do titular de dados. E assim por diante.

O enquadramento de uma atividade de tratamento em uma dessas bases legais finalísticas já demonstra que, ao menos aparentemente, o princípio da finalidade está sendo respeitado. Relembre-se que princípio da finalidade determina que para tratar dados pessoais exista uma finalidade definida: não se admite o tratamento de dados ao léu.

Assim, as hipóteses de tratamento finalísticas são categorias de finalidade, de modo que o agente de tratamento, ao enquadrar a sua atividade em uma dessas bases, já evidencia, ainda que de início, a observância ao princípio da finalidade. Segue-se ao enquadramento, por obrigação imposta pela LGPD, a identificação da finalidade específica.

Por exemplo, o tratamento de dados fundado em execução de contrato já explicita que na atividade de tratamento há um contrato celebrado e que esses dados serão tratados para o fim de cumprir as obrigações do pacto. Todavia, é necessário identificar essa finalidade específica, como “execução do contrato de prestação dos serviços médicos assinado entre o titular de dados e o controlador em 20/02/2020”. Nota-se: já se sabia que o tratamento se destinava à execução do contrato (categoria de finalidade), mas não se dispensa a identificação da finalidade (princípio da finalidade).

Consequentemente, o enquadramento da atividade em uma das bases finalísticas mostra um início de observância ao princípio da finalidade, o que não dispensa o controlador de identificar a finalidade do tratamento para dar integral cumprimento à referida norma.

Na outra mão, tem-se as bases legais de tratamento “não finalísticas”. As hipóteses de tratamento não finalísticas assim podem ser chamadas porque não demonstram, por si só, se há observância, ou ao menos início de observância do princípio da finalidade. São elas: consentimento e legítimo interesse.

O controlador, ao enquadrar uma atividade de tratamento no “consentimento” não explica, nem de início, para que ocorrerá o tratamento dos dados pessoais. O que se sabe, apenas, é que houve consentimento, mas não qual é o fim desse consentimento.

O mesmo ocorre para o legítimo interesse (autorizado apenas aos dados simples, ressalta-se). Observando-se todos os requisitos exigidos para o tratamento com fundamento nessa base, não se pode depreender, por si só, qual é a finalidade do tratamento, mas apenas que o tratamento se dará por legítimo interesse do controlador. Não se sabe para quê.

Nesses casos, portanto, torna-se ainda mais relevante a precisa identificação do fim do tratamento dos dados pessoais, para que seja observado em sua ideal concepção do princípio da finalidade, uma vez que a demonstração da base legal que o autoriza nem sequer dá início do objetivo do tratamento.

Há, ainda, a necessidade de observar um requisito de ordem subjetiva para o tratamento dos dados pessoais. É preciso verificar se o titular dos dados é menor ou não, tendo em vista que a LGPD estabelece um regime próprio para tratamento de dados pessoais de crianças e adolescentes, na forma do Art. 14.

O tratamento dos dados pessoais de crianças e adolescentes, portanto, só pode ocorrer em duas: quando houver consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal; sem consentimento, quando a coleta for necessária para contatar os pais ou o responsável legal; para proteção do menor (BRASIL, 2018).

Isso quer dizer, com base nas conclusões já realizadas nesta seção, que para dar licitude ao tratamento de dados de crianças e adolescentes, primeiro, é necessário verificar se os Arts. 7º e 11 o autorizam e, caso o autorizem, deve haver consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, ou, deve haver necessidade para contatar os pais ou o responsável legal, ou deve-se estar diante de situação que demande o tratamento para proteção da criança ou adolescente.

Portanto, para tratamento dos dados de menores, além das bases legais, deve haver preenchimento de ao menos um dos três requisitos específicos depreendidos do Art. 14 da LGPD, cuja inobservância, ainda que haja enquadramento nos Arts. 7º ou 11, provocará ilegalidade no tratamento dos dados.

Em conclusão, tratar dados pessoais somente será lícito se a atividade se enquadrar nas hipóteses taxativas dos Arts. 7º (dados pessoais simples) e 11 (dados pessoais sensíveis) da LGPD, a poder haver mais de uma base legal para o tratamento e, em caso de tratamento de dados sensíveis, será obrigatório identificar a base legal de tratamento dos dados pessoais simples.

Ademais, as bases legais de tratamento podem ser finalísticas ou não finalísticas. Aquelas, são as bases legais que demonstram, por si só, o início de observância ao princípio da finalidade, tendo em vista que as hipóteses de tratamento se caracterizam como categorias de finalidade. Estas, por sua vez, não conferem qualquer norte quanto à finalidade do tratamento dos dados.

Por fim, para o tratamento dos dados pessoais de crianças de adolescentes, deve-se cumprir o enquadramento do tratamento em ao menos uma das bases legais dos Arts. 7º e 11, e somar, ainda, o preenchimento de pelo menos um dos três requisitos para tratamento de dados de menores, dispostos no Art. 14 da LGPD.

3.5 Segurança e boas práticas

O Capítulo VII da LGPD se dedica a dispor sobre medidas de segurança e de sigilo de dados (Seção I) e sobre a adoção de boas práticas e de governança (Seção II). Tratam-se de diretrizes gerais a serem incorporadas pelos agentes de tratamento em suas atividades, de forma que os dispositivos do referido Capítulo visam expor o mínimo razoável esperado daqueles que promovem atividades de tratamento de dados pessoais.

Dessa forma, os Arts. 46 a 49 regem sobre a segurança e o sigilo de dados, cujo fim é impor que os agentes de tratamento, em qualquer das fases do tratamento dos dados pessoais, adotem mecanismos de segurança da informação a fim de proteger os dados pessoais.

Nesse sentido, o Art. 46, em seu *caput* prevê:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de

> destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

Note-se que esse dispositivo aborda exatamente sobre a segurança dos dados pessoais, que constitui um dos princípios da proteção dos dados pessoais, na forma da LGPD, Art. 6º, inciso VII. Logo, a Seção I tem por fim trazer concretude à norma principiológica enunciada no início da Lei. Ou seja, "[...] quem se propõe a tratar dados deve possuir, efetivamente, a capacidade de protegê-los, evitando ataques e acessos desautorizados, como forma de garantia de segurança das informações coletadas" (LOPES, 2019, p. 175).

Desse modo, note-se que as medidas técnicas "[...] são aquelas adotadas no âmbito da Tecnologia da Informação, com o uso de recursos informáticos dotados de funcionalidades voltadas à garantia da segurança da informação" (JIMENE, 2019, p. 329), enquanto as medidas administrativas "[...] são as atividades realizadas no âmbito administrativo-gerencial dos agentes de tratamento, incluindo-se as de natureza jurídica" (JIMENE, 2019, p. 330).

Ademais, a segurança da informação deve abranger tanto os meios eletrônicos, conectados ou não à internet, bem como os meios digitais, de forma que se deve considerar o tratamento de dados em meios físicos, como arquivos, fichas, pastas (COTS; OLIVEIRA, 2018, p. 240). Até porque, a LGPD é clara quando dispõe em seu Art. 1º que se aplica, "inclusive nos meios digitais" (BRASIL, 2018), de sorte a não haver qualquer dúvida quanto à aplicação ao tratamento de dados em meios não digitais.

A ANPD pode, ainda, consoante o § 1º do Art. 46, regulamentar de forma específica sobre padrões de segurança mínimos, tanto técnicos quanto administrativos, considerando a natureza dos dados, as características do tratamento, o estado atual da tecnologia, principalmente quanto aos dados sensíveis, bem como a ter por norte os princípios de proteção de dados pessoais (BRASIL, 2018).

> Ainda, constata-se que o legislador optou por adjetivas como "mínimos" os padrões técnicos que a ANPD poderá dispor, deixando claro que não se espera o uso de absolutamente todas as ferramentas tecnológicas existentes ou que venham a existir para garantir a segurança dos dados pessoais, situação que seria inviável, inclusive do ponto de vista econômico (JIMENE, 2019, p. 333).

De se depreender, assim, que as regulações por parte da ANPD não podem exigir dos agentes de tratamento que adotem medidas de segurança técnicas ou administrativas que extrapolem o mínimo razoável para a segurança dos dados

pessoais, sob pena de inviabilizar a atividade do agente de tratamento por exorbitar a onerosidade aceitável que medidas de segurança mínimas demandariam.

Por sua vez, o § 2º do Art. 46 dispõe categoricamente sobre o conceito de *privacy by design* (privacidade desde a concepção) criado por Ann Cavoukian, cujo objetivo é orientar que a privacidade deve compor a própria arquitetura de qualquer produto ou serviço, ou seja, a privacidade deve ser o ponto de partida para o seu desenvolvimento: "[a]s medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução" (BRASIL, 2018).

Cots e Oliveira (2018, p. 242-243) exemplificam as vantagens de se adotar a privacidade desde a concepção:

> Vamos utilizar um exemplo de outra área, mas bastante esclarecedor. Imaginemos um arquiteto que foi contratado para projetar uma casa. O profissional vai desenhando suas formas com liberdade, privilegiando iluminação natural e ventilação, espaços abertos, perspectivas etc. Todavia, não sabia o arquiteto, em nosso exemplo, que a casa seria construída em um bairro com alto índice de criminalidade. Após construída, a casa foi invadida diversas vezes, obrigando o arquiteto a prever medidas de segurança suplementares que, por serem adaptações, diminuíram consideravelmente a qualidade do projeto e a beleza da construção, além de serem menos eficientes do que se tivessem sido projetadas na construção original. Assim como o caso do exemplo, pensar na privacidade como premissa ou pressuposto do desenvolvimento de um produto ou serviço pode fazer com que ele seja mais eficiente e barato, pois não dependerá de adaptações posteriores.

Desenvolvido ainda na década de 1990, o conceito de *privacy by design* possui sete princípios fundamentais: (i) é proativo e não reativo, e é preventivo e não reparativo; (ii) a preservação da privacidade é o padrão (*privacy by default*) de configuração do produto ou serviço (e não o contrário, em que, no início, há exposição que pode ser cessada pelo usuário); (iii) a privacidade é incorporada no próprio desenho; (iv) a funcionalidade deve ser integral de forma a somar para todos os sujeitos envolvidos, agentes de tratamento e titulares de dados, de modo a não se escolher entre segurança e privacidade, que devem coexistir; (v) garantia de segurança da informação durante todo o ciclo de vida do tratamento dos dados, desde a coleta até a sua destruição/eliminação; (vi) transparência aos titulares de dados sobre as políticas de governança em proteção de dados adotadas pelos agentes de tratamento; (vii) respeito à privacidade dos usuários, que deve se sobressair em

relação aos outros interesses envolvidos, sendo, portanto, o elemento central (INFORMATION..., 2011).

De forma a complementar o Art. 46 da LGPD, o Art. 49 ainda dispõe que: “Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares” (BRASIL, 2018).

Nesse sentido, referido dispositivo reforça o que já se observa dos demais dispositivos da LGPD, como os seus fundamentos, os princípios, incluindo o da boa-fé, as bases de tratamento, e todas as demais normas que se pode extrair da LGPD, mas se releva, sobretudo, por apontar especificamente que eventuais normas regulamentares deverão ser atendidas pelos agentes de tratamento, em referência “[...] demais normas existentes ou que serão criadas no âmbito jurídico que complementarão ou dialogarão com a LGPD, no estabelecimento de regras com orientações mais específicas sobre determinados assuntos” (JIMENE, 2019, p. 349).

Na esteira do princípio da transparência, o Art. 48 dispõe sobre a comunicação à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança com potencial de causar riscos ou danos relevantes aos titulares de dados, que deverá ser comunicado em prazo razoável e deve conter, conforme § 1º do Art. 48:

> I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (BRASIL, 2018).

E nesse sentido, conforme o § 2º do Art. 48, ao analisar o incidente de dados, a ANPD poderá, ou seja, a seu critério, com base na gravidade que envolva o incidente, se necessário para preservação dos direitos dos titulares, determinar providências a serem adotadas pelo controlador, por exemplo, a ampla divulgação do incidente nos meios de comunicação e a adoção de medidas para diminuir os efeitos do incidente (BRASIL, 2018).

Ainda sobre a gravidade do incidente, o § 3º do Art. 48 prevê: “[...] será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas

que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los" (BRASIL, 2018).

Dessa forma, a LGPD impõe um modelo de adoção de medidas de segurança para proteção dos dados pessoais, sendo elas técnicas e administrativas-gerenciais da atividade de tratamento, as quais já deveriam ser observadas por mandamento do princípio da segurança, conforme impõe o Art. 6º, inciso VII, mas que são, ainda, objeto de análise mais detalhada na Seção própria.

O que se observa, porém, é que a despeito da melhor explanação sobre os procedimentos de segurança e as medidas a serem tomadas pelo controlador em caso de incidentes de dados, bem como sobre as posturas que podem ser exigidas pela ANPD, o verdadeiro detalhamento das medidas de segurança ficou a cargo de regulamentação própria pela ANPD.

Outrossim, a Seção II do Capítulo VII da LGPD aborda as boas práticas e a governança, de forma que no Art. 50 estabelece a possibilidade de os próprios agentes de tratamento elaborarem, individualmente ou coletivamente, regras padronizadas que demonstrem boas práticas e governança sobre tratamento de dados pessoais:

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

Segundo Lopes (2019, p. 183), "a seção ora analisada é corolário lógico dos princípios da segurança e da prevenção, conforme apresentados pelo legislador como axiomas basilares da proteção de dados". Desse modo, referidas boas práticas e governança dos dados pessoais têm como escopo principal conferir segurança ao tratamento dos dados e incorporar na prática dos agentes de tratamento medidas que visem prevenir a ocorrência de incidentes de dados pessoais.

Os §§ 1º, 2º e 3º do Art. 50 da LGPD conferem maior detalhe sobre o estabelecimento das boas práticas, cujo conteúdo é autoexplicativo, conforme indicado por Cots e Oliveira (2018, p. 252):

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

Relevante destacar, aqui, dois aspectos. O primeiro, é que a LGPD se preocupa com a estrutura de processamento de dados do controlador, de forma que expressamente indica (§ 2º) que os critérios de estrutura, volume de operações, sensibilidade, probabilidade e gravidade de danos para os titulares devem nortear o programa de governança de proteção de dados. Conforme Jimene (2019, p. 350) aponta “[...] é fácil compreender que não seria razoável estabelecer para uma padaria as mesmas normas de segurança que são estabelecidas para um hospital [...]”.

Em segundo lugar, a adoção de boas práticas e os critérios de segurança empregados no tratamento dos dados pessoais, e que devidamente comprovados, são circunstâncias a serem sopesadas para a imposição das penalidades previstas na LGPD. “A adoção de boas práticas é um dos itens que são considerados no

momento da imposição de sanções administrativas, que podem variar de advertência à multa de 50 milhões" (COTS; OLIVEIRA, 2018, p. 252).

Por fim, quanto à Seção II relativa às boas práticas, o Art. 51 ainda normatiza que "[a] autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais" (BRASIL, 2018). Aqui, nota-se novamente a LGPD impor regramento específico pela ANPD.

A finalidade desse regramento pode ser entendida como a imposição aos agentes de tratamento de adoção de soluções tecnológicas a serem utilizadas para dar maior controla aos titulares de dados, por exemplo, a utilização de aplicação por meio do qual o titular de dados possa exercer os seus direitos previstos no Art. 18.

Logo, observa-se que as boas práticas devem ser promovidas pelos agentes de tratamento a fim de dar concretude aos princípios da segurança e prevenção, de modo a demonstrar uma verdadeira alteração da estrutura administrativa das atividades do agente de tratamento, de modo a incorporar o tema da privacidade nas rotinas da corporação.

A adoção das boas práticas deve ser norteada por todas as disposições da LGPD, mormente por seus fundamentos e princípios e de modo a respeitar os direitos dos titulares, sendo que, para futura apuração de responsabilização do agente de tratamento acerca da ocorrência de incidentes de dados, as práticas adotadas pela organização serão critério para a imposição de sanção administrativa mais ou menos gravosa.

3.6 Autoridade Nacional de Proteção de Dados

A instituição de uma autoridade de proteção de dados é indispensável para garantir a autodeterminação informativa, isso porque a simples atuação individual na defesa da proteção dos dados não se mostra eficaz diante da desproporcionalidade que existe entre o titular de dados e toda a estrutura de um agente de tratamento voltada a tratar os dados pessoais e, ainda, preparada para impor restrições ao titular de dados caso opte por não fornecer suas informações (DONEDA, 2019, p. 320).

Desse modo, não bastaria a concepção de um sistema normativo complexo e detalhado, com a previsão de diversos direitos dos titulares de dados, fundamentos e principiologia própria a ser observada por controladores e operadores, se a tutela dos direitos fosse limitada à reclamação individual, sem respaldo de um ente próprio para equilibrar as relações entre os titulares de dados e os agentes de tratamento.

Para Doneda (2019, p. 320), “[...] tal tutela singular reproduziria uma tradição elitista da privacidade, que não corresponde à sua atual posição na nossa carta constitucional nem referencia outros direitos que devem ser mensurados nessa situação”, é dizer, sem uma autoridade de proteção de dados, a matéria não seria abordada sob o caráter fundamental que possui, mormente porque a proteção da privacidade é resguardada como direito fundamental na CF.

O texto final do projeto da LGPD autorizava a criação a ANPD, sob a natureza de autarquia vinculada ao Ministério da Justiça, que seria assessorada por um Conselho Nacional, todavia, ambos (ANPD e Conselho) foram vetados pelo então Presidente Michel Temer, diante da discussão havida quanto à legalidade do processo legislativo, tendo em vista que a criação de estruturas administrativas constitui atribuição exclusiva do Poder Executivo (GUTIERREZ, 2019, p. 393).

Nesse sentido, o veto se justificou diante da insegurança jurídica que poderia trazer face a possibilidade de futura decretação de inconstitucionalidade, por violação ao Art. 61, § 1º, inciso II, alínea “e” e ao Art. 37, XIX da CF. Por essa razão, o Presidente Michel Temer prometeu o envio de uma Medida Provisória ou de um Projeto de Lei para suprir a falta da ANPD (GUTIERREZ, 2019, p. 394).

Assim, a Medida Provisória 869 de 28 de dezembro de 2018 foi adotada para criar a ANPD e o Conselho Nacional de Proteção de Dados, suprindo, portanto, a omissão trazida pelo veto diante de sua redação original, e posteriormente a Medida Provisória foi transformada na Lei 13.853 de 8 de julho 2019, que modificou a LGPD para incluir os seus dispositivos.

Tema de forte debate relativo à ANPD é a sua independência, assunto este que ainda se faz latente por ter sido a ANPD trazida sob a natureza de órgão da administração pública federal, integrante da Presidência da República, portanto, sem ao menos personalidade jurídica própria.

Em sentido totalmente contrário à configuração atual da ANPD, orientou Doneda (2019, p. 321), expressamente, que tal autoridade “[...] não deva estar diretamente vinculada a um dos poderes pelas próprias consequências da ausência de independência desse órgão quando submetido à estrutura hierárquica da administração pública direta”.

Conforme explica Gutierrez (2019, p. 399), o debate pela autonomia da autoridade de proteção de dados relaciona-se “[...] à necessidade de que a Autoridade de Proteção de Dados tenha autonomia e independência para regular e fiscalizar

somente as atividades de tratamento de dados pessoais pelo setor privado, mas também àquelas realizadas pelo poder público".

Parentoni (2019, p. 212) argumenta no mesmo sentido acerca do atual *status* da ANPD: "[...] em sua estrutura atual, a ANPD não teria independência suficiente para desempenhar satisfatoriamente as suas atribuições, mormente quando fosse necessário fiscalizar o próprio Poder Público".

Retoricamente questionam Vasconcelos e de Paula (2019, p. 732): "Se o ente perdeu importante parcela de sua autonomia e independência, [...] como garantir que haverá proteção de direitos individuais frente à atuação do próprio Poder Público?".

Portanto, a independência da ANPD se justifica porque seu escopo não se restringe à regulamentação e fiscalização das atividades de tratamento da esfera privada, mas se estende, igualmente, conforme as previsões da LGPD, ao poder público, de modo que tão somente independência poderia assegurar a atuação da ANPD sobre os entes públicos.

Corrobora Doneda (2019, p. 321):

> Conforme verificamos, o escopo da tutela a qual visa esse órgão supõe uma neutralidade frente às próprias razões de Estado, o que seria inatingível sem sua independência. Note-se que o Estado – e, em particular, o poder executivo – apresenta demasiado interesse na coleta e processamento de dados pessoais para que essa sua atividade possa harmonizar-se com a proteção desses mesmos dados, ao menos com a isenção hoje pretendida e necessária.

Quanto ao tema, o Art. 55-A, §§ 1º e 2º da LGPD dispõe que a natureza jurídica de órgão da administração pública federal é transitória, de modo que pode ser transformada em entidade submetida a regime autárquico especial, e que essa transformação deverá ser avaliada dentro do prazo de dois anos da entrada em vigor do atual regime da ANPD (BRASIL, 2018).

A despeito da sua atual estrutura e das críticas inerentes a essa configuração, o Art. 55-B, a fim de atender, ainda que limitadamente, essa demanda por independência da ANPD, prescreve: "É assegurada autonomia técnica e decisória à ANPD" (BRASIL, 2018).

Assegurada a independência técnica e decisória da ANPD, garante-se, ao menos, que seus atos serão imperativas e não passíveis de revisão por demais órgãos superiores ou diversos da administração, de modo que tão somente poderão ser revistos mediante provocação do Poder Judiciário.

Adiante, a estrutura da ANPD está disposta nos Arts. 55-C e 55-D da LGPD, de forma que neste primeiro dispositivo apresenta os seus órgãos de composição: Conselho Diretor; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Corregedoria; Ouvidoria; órgão de assessoramento jurídico próprio; unidades administrativas especializadas necessárias à aplicação da LGPD (BRASIL, 2018).

Já as funções da ANPD estão dispostas no Art. 55-J, em um total de vinte e quatro incisos, que podem ser aglomerados, em cinco categorias de funções: fiscalizadora-sancionadora; educativa, de conscientização e fomentadora do debate sobre proteção de dados pessoais; atenção direta ao titular de dados; normativo-interpretativa; transparência da auto-gestão.

A função fiscalizadora-sancionadora comporta a competência para fiscalizar a observância pelo setor privado e também pelo setor público, do cumprimento das disposições da LGPD, a poder a ANPD, ainda, solicitar informações dos agentes de tratamento a fim de averiguar a observância à proteção de dados pessoais, a poder, ainda, informar órgãos e autoridades sobre a prática de crimes e ilícitos envolvendo a proteção de dados pessoais e, por fim, comporta que a ANPD aplique sanções por violação à LGPD, conforme autorizam os Arts. 52 a 54 desta Lei.

Por sua vez, a função educativa, de conscientização e fomentadora do debate sobre proteção de dados pessoais norteia a atuação da ANPD no sentido de ser ente protagonista para promover a transformação cultural que impõe o novo paradigma de proteção de dados que a LGPD estatui, tanto para educar a conscientizar os titulares de dados quanto os agentes de tratamento, que também devem participar do debate.

A atenção direta ao titular de dados atribui à ANPD a competência para receber por meio de canais diretos, as reclamações do titular de dados contra o controlador. Aqui, verifica-se notadamente o objetivo de equalizar as forças do titular de dados e dos agentes de tratamento, o que é feito, portanto, por meio da recepção das reclamações contra estes na hipótese em que descumprem as solicitações pertinentes aos direitos dos titulares nos prazos estabelecidos.

Já a sua função normativo-interpretativa decorre, além dos incisos específicos do Art. 55-J, de outros diversos dispositivos em todo o corpo da LGPD que lhe atribuem a função de pormenorizar temáticas que são abordadas de forma genérica e principiológica no decorrer da Lei.

Por fim, a função de transparência da auto-gestão confere à ANPD o dever de relatar suas atividades, bem como arrecadar receitas e emprega-las, de modo a detalhar o emprego dos recursos em suas atividades por meio de relatórios.

Para facilitar a compreensão, apresenta-se o seguinte quadro com a subdivisão das funções da ANPD nos termos das categorias elencadas:

Funções da ANPD – Art. 55-J da LGPD	
Fiscalizadora-sancionadora	I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;
Educativa, de conscientização e fomentadora do debate sobre proteção de dados pessoais	III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

	XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
Atenção direta ao titular de dados	V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.
Normativo-interpretativa	X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;
Transparência da auto-gestão	XII - elaborar relatórios de gestão anuais acerca de suas atividades; XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

Logo, é nítido que a ANPD possui papel fundamental para promover a observância à LGPD, por meio da fiscalização de seu cumprimento, aplicação de sanções, a mudança da cultura, tanto das organizações, privadas e públicas, quanto dos próprios titulares de dados e, assim, deve atuar como autoridade protagonista a fim de conscientizar e educar a sociedade frente ao novo paradigma jurídico de proteção de dados pessoais que traz a LGPD.

Deste capítulo, portanto, embora não se tenha analisado a LGPD à exaustão, pode-se observar que o novo sistema jurídico de proteção de dados pessoais detém instrumentos muito específicos e, ainda, que possui normas de ampla aplicação, com vistas a perseguir o escopo da LGPD no sentido de garantir ao titular de dados a proteção de seus direitos fundamentais de liberdade, privacidade e livre desenvolvimento de sua personalidade.

Os fundamentos e a principiologia abarcados na LGPD devem ser o norte abstrato a ser concretizado em cada circunstância e ser avaliada pelo DPO, seja no exercício de direitos pelo titular de dados ou no cotidiano nas atividades de tratamento de dados pessoais. As bases legais, nesse sentido, devem sempre fundamentar o tratamento dos dados pessoais, segundo boas práticas de segurança, inclusive. E, assim, caberá à ANPD, dentre as suas diversas funções, zelar pela observância à LGPD, ao que deverá responder o DPO, como intermediário da organização em que assim funcionar. Por conseguinte, diante deste cenário normativo ora observado, aborda-se a moldura jurídica pertinente ao DPO.

4 O *DATA PROTECTION OFFICER* NA LGPD SOB O PARADIGMA DA GDPR

Como é o propósito deste trabalho, no presente capítulo se aborda a figura do encarregado de proteção de dados, assim definido na LGPD, chamado, comumente, de *data protection officer* ou *data privacy officer*, o DPO, devido à cultura já instituída de privacidade e proteção de dados importada de outros países, em especial, da Europa, em que hoje vige a GDPR, ou chamado, também de EPD (Encarregado de Proteção de Dados), em países como Portugal e Espanha.

Para delimitar a metodologia, se indica que este trabalho faz uso das referências ao DPO na GDPR naquilo em que é previsto em tal legislação para auxílio à abordagem dos temas adiante analisados, como no delineamento de suas funções. Assim, quando a GDPR prevê os temas abordados relacionados ao encarregado de proteção de dados, tais referência legislativas são mencionadas como premissas para as conclusões adiante realizadas. De outra mão, naquilo em que não houver disposição na GDPR, dispensa-se a análise comparada, valendo-se este trabalho das referências do Direito brasileiro em suas diversas fontes.

4.1 Origem e atual *status* na GDPR e na LGPD

O encarregado pelo tratamento de dados não é uma figura nova, nem na GDPR, nem na LGPD. Se origina, na verdade, na Lei Federal Alemã de 1977, especificamente na Seção 38, e em tal diploma legislativo permanece até hoje, em complemento com a GDPR, no Direito alemão.

Além disso, também estava incorporado na Diretiva 46 de 1995 do Conselho Europeu, como condição para que os Estados-membro da União Europeia pudessem simplificar ou se isentar de notificações à Autoridade de Proteção de Dados, conforme Art. 18, item 2 (UNIÃO EUROPEIA, 1996):

> Os Estados-membros apenas poderão estabelecer a simplificação ou a isenção da notificação nos seguintes casos a condições: - se o responsável pelo tratamento nomear, nos termos do direito nacional a que está sujeito, um encarregado da proteção dos dados pessoais, responsável nomeadamente por - garantir, de modo independente, a aplicação, a nível interno, das disposições nacionais tomadas nos termos da presente directiva, manter um registro dos tratamentos efectuados pelo responsável do tratamento, contendo as informações referidas no nº 2 do artigo 21º, assegurando assim que os tratamentos não são susceptíveis de prejudicar os direitos e liberdades das pessoas em causa.

Na mesma Diretiva, o considerando 54 também fomenta a incorporação do DPO (UNIÃO EUROPEIA, 1995):

> Considerando que, de todos os tratamentos efectuados em sociedade, o número dos que apresentam tais riscos particulares deverá ser muito restrito; que os Estados-membros devem estabelecer um controlo prévio à realização desses tratamentos a efectuar pela autoridade de controlo ou pelo encarregado da protecção dos dados em cooperação com essa autoridade; que, na sequência desse controlo prévio, a autoridade de controlo pode, de acordo com o direito nacional, dar um parecer ou autorizar o tratamento dos dados; que esse controlo pode igualmente ser efectuado durante os trabalhos de elaboração de uma medida legislativa do parlamento nacional ou de uma medida baseada nessa medida legislativa, a qual defina a natureza do tratamento e especifique as garantias adequadas.

Dessa forma, a Diretiva incentivava a incorporação do encarregado de tratamento de dados para que atuasse em cooperação com a autoridade de controle, a fim de realizar a ponderação e controle prévios às atividades de tratamento, considerando os riscos do tratamento de dados potenciais à sociedade.

O que se nota, assim, é que a Diretiva 46 incentivava e trazia o DPO como uma figura facultativa ou alternativa em certas circunstâncias, como se observa, no Art. 18, a fim de flexibilizar as notificações à autoridade, desde que exercesse as funções ali estabelecidas, sendo aqui, portanto, alternativo, ou, conforme ponderado no considerando 54, como uma figura facultativa que pudesse atuar em cooperação com a autoridade de proteção de dados. É dizer, na Diretiva 46, não era obrigatória a instituição do DPO, mas facultativa ou alternativa.

Mais recentemente, a figura do DPO fica consagrada no Regulamento 45 de 2001 do Conselho Europeu, sobre tratamento de dados pessoais pelas instituições e órgãos comunitários e livre circulação desses dados, nos seus Arts. 24 a 26, de modo que trouxe uma definição detalhada do DPO a fim de atuar nessas entidades, agora em caráter obrigatório, a determinar que em cada instituição e órgão da comunidade europeia deve ser designado ao menos um encarregado de proteção de dados (UNIÃO EUROPEIA, 2001).

Ainda no Regulamento 45, são atribuídas diversas funções ao DPO, dentre elas, assegurar a informação aos titulares de dados, responder às solicitações da Autoridade Europeia de proteção de dados, manter o registro dos tratamentos de dados e notificar a Autoridade Europeia nas situações de tratamento que apresentarem riscos aos direitos e liberdades dos titulares de dados (UNIÃO EUROPEIA, 2001).

Na GDPR, o DPO está instituído nos Arts. 37, 38 e 39, como uma figura consolidada, em que há disposições sobre a necessidade de sua designação, ou seja, quando é obrigatória a sua indicação, a posição do encarregado de proteção de dados e, ainda, as suas funções, de forma relativamente pormenorizada (UNIÃO EUROPEIA, 2016), temas esses que serão a seguir detalhados.

Poder-se-ia imaginar que o DPO ou a sua situação na GDPR teria posição sem relevância devido ao reconhecimento em apenas três artigos, entretanto, tal circunstância não poderia levar a tal incorreção, tendo em vista que em todo o espírito da GDPR é possível depreender a verdadeira importância dessa figura (WOLTERS KLUWER, 2018).

De forma mais enxuta, a LGPD dispõe sobre o encarregado no seu Art. 5º, definindo-o, e adentra no tema de sua obrigatoriedade e funções no Art. 41. Nesse sentido, o Art. 5º, inciso VIII, assim define o DPO: “encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” (BRASIL, 2018).

Nesse sentido, a seguir se detalha os temas relativos ao DPO, na perspectiva da LGPD e do Direito brasileiro em geral, a se averiguar os principais temas correlatos a essa figura, em comparação com as disposições da GDPR, com o objetivo de compreender, efetivamente, os principais desdobramentos de sua atividade.

4.2 Funções

A previsão do DPO tem o objetivo de instituir dentro das organizações privadas e também dentro do poder público uma figura que seja um representante para fazer a intermediação com a Autoridade Nacional de Proteção de Dados (*Data Protection Authority*, na GDPR), também com os titulares de dados, e que, simultaneamente, seja uma figura que se ocupe de levar à organização o conhecimento e atualizações sobre proteção de dados pessoais e que se proponha, nesse sentido, a criar e manter uma cultura de observância às normas de proteção de dados pessoais nas atividades de tratamento da organização.

Como se observará adiante, das funções que lhe são atribuídas, o DPO se insere na organização, sob a ótica do Direito do Trabalho, como uma atividade-meio. Ora, a organização tem o seu fim, o seu objeto, por exemplo, comércio veículos, sendo o DPO, portanto, não um vendedor, mas atuante na proteção dos dados pessoais,

para que outros elementos, dentre eles, humanos, funcionem diretamente na atividade-fim, no caso, comércio, e que, portanto, devido à atividade-meio desempenhada pelo DPO, o fim da organização seja perseguido com observância à legislação sobre proteção de dados pessoais.

Nesse sentido, nos termos do Art. 41, § 2º, da LGPD estão estabelecidas as atividades a serem desempenhadas pelo DPO. São elas, portanto:

> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018).

As suas funções correspondem à definição que a LGPD confere ao DPO, no sentido de constituir um canal de comunicação entre o controlador e os titulares de dados e a Autoridade Nacional de Proteção de Dados, de modo que, assim, as suas atividades visam cumprir o motivo da sua própria concepção.

Portanto, para Mello (2019, p. 164), "[s]eu propósito é fomentar a proteção dos dados pessoais, atuando como canal de comunicação entre o controlador e as demais figuras instituídas pela LGPD (titular e ANPD), além de adotar providências, se necessárias". E, ainda, nessa linha, ensinam Cots e Oliveira (2018, p. 220) que "[a] primeira e a segunda atribuições são as mais básicas possíveis, se lembrarmos que, segundo o conceito legal, o encarregado é um meio de comunicação entre o controlador e terceiros".

Especificamente sobre o aceite de reclamações e comunicações dos titulares de dados e a prestação de esclarecimentos e tomada de providências, deve-se fazer um paralelo irremediável com o exercício dos direitos dos titulares, dispostos ao longo de toda a LGPD, mas sobretudo quanto àqueles previstos no Art. 18.

Por exemplo, note-se que se o titular de dados exercer o seu direito de confirmação, previsto no inciso I do Art. 18, a solicitar do controlador que informe se realiza o tratamento de seus dados, em tese, o DPO deve capitanear essa comunicação com o titular de dados, prestando-lhe suficientemente as informações solicitadas. Outro exemplo pode ser dado quanto ao direito de retificação, na medida em que o titular de dados pode solicitar ao controlador que corrija os seus dados devido a uma atualização ocorrida em seus dados pessoais, conforme prevê o inciso III do Art. 18.

Veja-se, ainda, que conforme normatiza o § 1º do Art. 19 da LGPD, os dados pessoais devem ser armazenados em um meio que facilite o exercício do direito de acesso, de modo que cabe ao DPO, frisa-se, capitanear medidas a fim de, na prática da organização, efetivamente facilitar o exercício de tal direito pelo titular de dados.

Destaca-se que se utiliza o termo “capitanear” para os exemplos mencionados tendo em vista que, dependendo da estrutura da organização, menor ou maior, o DPO poderá se caracterizar como um líder de um verdadeiro comitê de proteção de dados, ou seja, grupo de pessoas, inclusive podendo ser multifuncional, responsável pela observância da LGPD.

E é evidente que, sob pena de completa inviabilidade humana, grandes organizações não poderão deixar a cargo do DPO, uma só pessoa, a responsabilidade exclusiva pela comunicação com os titulares de dados, a exemplo de companhias de telefonia, que possuem milhões de clientes que podem ensejar milhares de solicitações diárias referentes aos seus dados pessoais.

Portanto, em grandes estruturas, certo é que as funções do DPO serão desenvolvidas não por uma só pessoa, mas por diversas pessoas que visem a observância da função do DPO quanto à comunicação com os titulares de dados, de modo a atendê-los e a adotar as providências que forem necessárias conforme impõe a LGPD.

Quanto à segunda função expressa do DPO, receber comunicações da ANPD e adotar providências, no que tange ao volume de trabalho que possa ser gerado devido ao tamanho da estrutura organizacional, as mesmas conclusões apontadas quanto à comunicação com os titulares de dados podem aqui, também, ser atribuídas.

Isso porque, da mesma forma que uma grande organização pode ensejar diversas solicitações de titulares de dados diariamente, poderá também receber constantes demandas da ANPD, não por irregularidade no tratamento dos dados, mas pelas particularidades que pode carregar o tratamento de dados, como uma grande operadora de seguro de saúde que trate comumente dados sensíveis, em grande volume e em nível nacional. Certo é que no caso de uma organização como esta da mesma forma seria humanamente impossível concentrar em uma só pessoa as respostas e esclarecimentos necessários à Autoridade Nacional.

E, nesse sentido, caberá ao DPO fazê-lo pessoalmente ou capitanear as comunicações com a ANPD, por exemplo, quando o Art. 31 da LGPD dispõe que na hipótese de violações poderá enviar informe com medidas cabíveis para cessar a

violação, ao DPO ou à equipe que exerça as suas funções, caberá responder ao referido informe, demonstrando a adoção de tais medidas, de forma dialogar com a ANPD.

Ainda, outro exemplo é, nos termos do Art. 10, § 3º da LGPD, a possibilidade de a ANPD solicitar ao controlador relatório de impacto à proteção de dados pessoais na hipótese em que realize tratamento de dados pessoais com fundamento na base legal de legítimo interesse, situação em que caberá ao DPO capitanear tal comunicação, mediante fornecimento do referido relatório e prestação de esclarecimentos sobre a atividade de tratamento de dados pessoais realizada.

Outro importante ato de comunicação está previsto no Art. 48 da LGPD, que impõe ao controlador a comunicação à ANPD na ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados, situação em que caberá ao DPO liderar referida comunicação, observando prazo razoável, e de modo a mencionar a natureza dos dados afetados, os titulares envolvidos, as medidas utilizadas para proteção de dados, os riscos relacionados ao incidentes, motivos da demora, se não comunicar o incidente de forma imediata, bem como as medidas que foram ou serão adotadas para mitigar os efeitos do incidente (BRASIL, 2018).

Assim, fica claro que o DPO é ponte, também, entre o controlador e a ANPD, de modo que, para isso, deve ter conhecimento teórico e prático das atividades de tratamento, de maneira a ter aptidão para cumprir todos os atos de comunicação e para responder à ANPD no que se refere às atividades da organização em que funciona.

Adiante, a terceira função do DPO consiste na orientação dos funcionários e colaboradores, com vistas a promover boas práticas relacionadas à proteção de dados pessoais. Segundo Cots e Oliveira (2018, p. 220), referida previsão demonstra que o DPO “[...] não é um mero relações públicas do controlador, pois só poderá ‘orientar’ funcionários e contratados se compreender minimamente a legislação incidente sobre a atividade, bem como os aspectos envolvidos no tratamento de dados”. Especificamente sobre a qualificação do DPO, se abordará em seção posterior.

O que se nota, assim, dessa terceira função expressamente disposta na LGPD, é que o encarregado de proteção de dados deve promover a cultura de proteção de dados, a orientar as boas práticas da organização, com vistas à observância da LGPD.

O DPO, nesse sentido, é inserido como uma verdadeira figura para fomentar as boas práticas que dispõe o Art. 50 da LGPD, e, evidentemente, na medida de sua função, que não se confunde com um *Chief Information Security Officer* (CISO) – diretor de segurança da informação –, também deverá zelar sobre boas práticas de segurança, até por obrigatoriedade de respeito aos princípios de segurança e prevenção, conforme Art. 6º, incisos VII e VIII da LGPD.

Por fim, no inciso IV do § 2º, do Art. 41, a LGPD dispõe como atividade do DPO "executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares". Desde já se ressalta que as demais atribuições a que se refere o inciso, diz respeito a atribuições relacionadas à proteção de dados pessoais, em consonância com a LGPD. Dessa forma, além das outras funções anteriormente previstas, outras, de temas correlatos, podem ser agregadas às atividades do DPO.

E isso se menciona porque a cumulação das funções do DPO, com vistas à aplicação da LGPD na organização, com outras funções diversas da proteção de dados pessoais, deve ser minuciosamente analisada para que não haja conflito de interesses entre a função diversa e a função de encarregado de proteção de dados. Especificamente sobre o conflito de interesses, se abordará adiante, em seção própria do tema.

A segunda parte do último inciso aqui analisado relega a atribuição de demais funções do DPO a normas complementares, que poderão, portanto, ser estabelecidas em Lei, ou pela própria ANPD, mediante regulamentação da matéria, conforme autoriza, em seguida, o § 3º do Art. 41 da LGPD: "A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado [...]".

Portanto, a LGPD elenca expressamente três funções a serem exercidas pelo DPO, o qual constitui um canal de comunicação entre o controlador e os titulares de dados bem como entre o controlador e Autoridade Nacional de Proteção de Dados, a dever promover os atos de comunicação que determina a LGPD, bem como responder às solicitações e fornecer informações aos titulares de dados e à ANPD, e, ainda, exerce o DPO o papel de fomentar a cultura de boas práticas de proteção de dados na organização, com o poder de orientar os funcionários e contratados sobre o tema.

Por seu turno, a GDPR elenca cinco funções do encarregado de proteção de dados no Art. 39, item 1. A primeira delas vai ao encontro da terceira função disposta na LGPD (UNIÃO EUROPEIA, 2016):

> a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

Veja-se, assim, que no inciso III, do § 2º, do Art. 41 da LGPD, o DPO deve orientar as boas práticas dos funcionários e contratados quanto à proteção de dados pessoais, sendo que o item a primeira função do item 1, do Art. 39 da GDPR está em consonância com o nosso ordenamento jurídico, podendo ser mencionada, de algum modo, como mais abrangente, por atribuir ao DPO informar e aconselhar o próprio responsável pelo tratamento, e não só seus funcionários e contratados, todavia, em termos práticos, a finalidade é a mesma, porquanto quem realiza o tratamento de dados são as pessoas que funcionam, sob qualquer cargo, em favor do agente de tratamento.

Adiante, a segunda função do DPO na GDPR (UNIÃO EUROPEIA, 2016):

> b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

Desse modo, o que deve promover o DPO é a observância ao GDPR nas atividades de tratamento de dados pessoais, além de todas as demais normas que visem o mesmo desiderato, inclusive para os fins de promover a formação dos colaboradores envolvidos com tratamento de dados pessoais, além de, também, controlar auditorias sobre a matéria.

Conforme orienta o Conselho Europeu (2017), diante de tais funções, o DPO está autorizado a: “recolher informações para identificar as atividades de tratamento; analisar e verificar a conformidade das atividades de tratamento; prestar informações e aconselhamento e formular recomendações ao responsável pelo tratamento ou ao subcontratante”.

Tal disposição, da mesma maneira que a anterior, poder-se-ia dizer mais abrangente que as funções do DPO previstas na LGPD, todavia, em suma, o que essa

segunda função da GDPR dispõe é que o encarregado deve promover o respeito à proteção de dados, em todos os níveis, e envolvendo qualquer funcionário ou contratado que participe da atividade de tratamento, conclusão esta a que se pode chegar, também, mediante análise do inciso III, § 2º, do Art. 41 da LGPD, tendo em vista que este dispõe sobre o poder de orientar tanto os funcionários quanto os contratados em relação à proteção de dados, de forma que qualquer pessoa, física ou jurídica, que venha a manter qualquer relação contratual com o controlador, pode se sujeitar às orientações do DPO sobre proteção de dados.

A terceira função do DPO na GDPR não está expressamente prevista na LGPD, entretanto, consoante se abordará em seguida, sob o espírito e principiologia da LGPD, à mesma conclusão se poderia chegar: “Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.o” (UNIÃO EUROPEIA, 2016).

No regime da GDPR, é obrigatória a elaboração de relatório de impacto na hipótese em que a atividade de tratamento possa gerar elevado risco para os direitos e liberdades das pessoas naturais, conforme prevê seu Art. 35. É aqui, portanto que atua o DPO consoante a função acima exposta, de maneira a aconselhar a avaliação de impacto e a controlar a sua formatação.

Ora, nesse sentido, se, nos termos do inciso III, § 2º, do Art. 41 da LGPD, cabe ao DPO orientar as boas práticas sobre proteção de dados pessoais, cabe a este, inclusive, fazê-lo quando da necessidade de elaboração de relatórios de impacto – sem aqui se adentrar à discussão quanto à necessidade ou não de tais relatórios em determinadas situações específicas.

As funções quarta e quinta do DPO na GDPR, por fim, são as que seguem (UNIÃO EUROPEIA, 2016):

> d) Coopera com a autoridade de controlo; e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.o, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

Desse modo, o DPO, na GDPR, constitui um meio para contato com a Autoridade de Proteção de dados, e com esta deve cooperar, o que está em consonância com a mesma função definida na LGPD, inciso II, § 2º, do Art. 41 da LGPD.

A despeito de a LGPD não prever expressamente a “cooperação” do DPO com a ANPD, qualquer conclusão que não seja cooperar com a Autoridade seria

antijurídica, contrária a todo o propósito da LGPD, seus fundamentos, princípios e demais disposições.

Devido à própria função da ANPD, que deve fiscalizar a aplicação da LGPD, não haveria como se esperar postura do DPO que não fosse cooperativa, até porque, se este deve zelar pelas boas práticas no tratamento dos dados pessoais e se, obviamente, deve zelar pela observância à LGPD, inclusive, sob o prisma do princípio da boa-fé, conforme impõe o *caput* do Art. 6º da LGPD, uma postura cooperativa é legitimamente esperada do desempenho de suas funções.

Ainda, importante abordar a função do DPO de realizar a consulta prévia e qualquer tipo de consulta junto à Autoridade, consoante define a quinta função do encarregado de dados na GDPR. A consulta prévia específica que designa diz respeito à consulta à Autoridade quando a avaliação de impacto de uma atividade de tratamento concluir por elevado risco caso não sejam tomadas medidas de atenuação pelo responsável do tratamento.

Aqui, de novo, o DPO, ao encontro do que prevê o inciso II, § 2º, do Art. 41 da LGPD, atua como um canal para comunicação com a Autoridade. No mesmo sentido, também se pode verificar correspondência com o inciso III, § 2º, do Art. 41 da LGPD, devido à função de promover as boas práticas. Do que se conclui, assim, que na hipótese de consultas junto à ANPD, poderá o DPO, nos termos da LGPD, também assim funcionar.

Pode-se concluir que o inciso III, § 2º, do Art. 41 da LGPD configura uma disposição chamariz sobre a atuação do DPO, de forma que lhe atribui, portanto, ampla função para orientar as atividades de tratamento de maneira abrangente na organização, de modo que serve como conselheiro para a tomada de decisão sobre qualquer assunto que se relacione à proteção de dados pessoais.

Interessante, inclusive, que o Art. 5º, inciso VIII, da LGPD, quando define o encarregado de proteção de dados, o faz sob o prisma de que servirá como um comunicador entre o controlador e os titulares de dados e a ANPD. Entretanto, ao se analisar de maneira mais detalhada o inciso III, § 2º, do Art. 41 da LGPD, inclusive em análise comparada com as funções definidas na GDPR, depreende-se de maneira muito clara que a atuação do DPO é abrangente, sempre com vistas à aplicação de todas as normas sobre proteção de dados pessoais, previstas na LGDP ou não, que assegurem as boas práticas da organização sobre a matéria.

Além disso, o que se observa é que as funções até então previstas para o DPO na LGPD não são mais restritas que as funções dispostas na GDPR, porquanto ao se realizar a leitura das funções estabelecidas no § 2º do Art. 41 em conformidade com os demais dispositivos da LGPD, como os seus princípios, fundamentos, boas práticas, direitos dos titulares, estas estão em equivalência com as funções atribuídas ao encarregado de proteção de dados na GDPR, e, assim, não deixam a desejar frente à norma europeia.

Ainda, importante ponderar o que o DPO não é. Pelo próprio conceito, o DPO será encarregado do tratamento de dados pessoais, de modo a desempenhar suas funções relativas à comunicação com a ANPD e com os titulares de dados, e, ainda, a servir como um fomentador da observância da LGPD pela organização, o que não lhe impõe um papel de analista de dados.

Ao ter o dever de promover a proteção dos dados pessoais tratados na organização, não lhe impõe analisar e acessar o conteúdo das operações de tratamento de dados pessoais, e, sim, auxiliar, como encarregado pela proteção dos dados pessoais, nas decisões que serão tomadas relacionadas à matéria.

Isso porque, admitir que o DPO seja pessoa que terá acesso ao conteúdo das operações tratamento de maneira livre, tão somente por sua posição de DPO, não parece observar os princípios da segurança e da prevenção, conforme Art. 6º, incisos VI e VII da LGPD. Além disso, conflitaria também com o Art. 46 da LGPD, que determina o contrário, ou seja, a imposição de adoção de medidas de segurança, técnicas e administrativas, para que não haja acesso de qualquer maneira inadequada.

Logo, o DPO não se confunde com um analista de dados, de forma que não constitui sua função analisar, uma a uma as operações de tratamento em relação ao seu conteúdo, tendo acesso livre e irrestrito, compreensão esta em consonância com os princípios da segurança e da prevenção e que evidencia a efetiva adoção de boas práticas de segurança.

O norte estabelecido, assim, é no sentido de que o DPO seja o ponto focal da empresa sobre proteção de dados e que lide no dia a dia com as solicitações dos titulares de dados e da ANPD, de forma a zelar de forma ampla pela observância da LGPD no tratamento de dados operado pela organização. Seu papel é de aconselhar, recomendar, e não necessariamente terá papel decisório sobre as políticas da organização quanto ao tratamento de dados.

4.3 Pessoa natural ou jurídica, suas qualificações e a sua publicização

A LGPD, em sua redação original, designava que o DPO seria, conforme Art. 5º, inciso VIII: “pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional” (BRASIL, 2018). O destaque aqui, portanto, é a indicação da pessoa “natural”, a qual, todavia, foi alterada posteriormente, como se verá.

Em obra publicada antes da alteração legislativa, Cots e Oliveira (2018, p. 219), a respeito de tal definição, indicaram: “[...] já se depreende que o encarregado deverá ser uma pessoa natural, ou seja, uma pessoa de carne e osso, estando vedada a contratação de pessoas jurídicas para esse fim”.

Anotaram, entretanto, um importante aspecto que, a despeito da revisão desse dispositivo, serve para a conclusão apresentada ao final, ao consignarem que apesar de ter indicado a necessidade de o DPO ser uma pessoa natural, não houve a imposição de um vínculo de emprego na contratação do encarregado, de forma que a contratação poderia se dar na forma de uma consultoria especializada (COTS; OLIVEIRA, 2018, p. 219).

Acontece que a Medida Provisória 869, que também instituiu a ANPD, alterou a redação da definição do DPO, de forma a suprimir a designação “natural” para deixar aberta a atuação do DPO tanto a pessoas naturais quanto a pessoas jurídicas, de forma a indicar, a nova redação do Art. 5º, inciso VIII: “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” (BRASIL, 2018).

Foi nítido o objetivo da Medida Provisória, posteriormente convertida em Lei, no sentido de permitir tanto a pessoas físicas quanto jurídicas o exercício da atividade de *data protection officer* ao suprimir o termo “natural” da definição do encarregado de proteção de dados. Ora, o Código Civil trata em seu Livro I das pessoas, e em seus respectivos títulos I e II, das pessoas naturais e das pessoas jurídicas, respectivamente (BRASIL, 2002), de maneira que, em Direito, quando se designa pessoa, esta poderá ser tanto a pessoa natural/física quanto a pessoa jurídica.

A GDPR, por seu turno, não especifica de forma expressa se o DPO deverá ser pessoa natural ou jurídica, todavia, a interpretação conferida pelo próprio Conselho Europeu, nas orientações sobre os encarregados da proteção de dados,

menciona a possibilidade de exercício externo da função, com base em um contrato de prestação de serviços, desde que todas as pessoas que funcionem nessa organização como DPO, preencham os requisitos objetivos exigidos na GDPR para a nomeação do encarregado de proteção de dados (CONSELHO..., 2017).

O Conselho Europeu (2017) ainda aponta as vantagens dessa configuração do DPO: “Simultaneamente, as competências e os pontos fortes individuais podem ser combinados de modo que várias pessoas, trabalhando em equipa, possam servir os seus clientes de forma mais eficiente”.

Essa figura do DPO externo, terceirizado, se tornou popularmente conhecida como DPO *as a service*, o que significa, portanto, o DPO como um serviço, a consistir em um serviço comum na Europa, em que empresas especializadas se propõem a exercer as funções de DPO em prol da organização.

Ainda, sobre o exercício da função de DPO por uma empresa externa, terceirizada, orienta o Conselho Europeu (2017) que para fins de clareza jurídica e de boas práticas, essa organização que exerça o papel de encarregado de proteção de dados deve indicar um membro específico da equipe responsável por cada cliente.

Logo, se conclui que a LGPD, em sua redação atual, permite que tanto pessoas naturais quanto pessoas jurídicas possam desempenhar o papel de encarregado de proteção de dados, o que segue, nesse sentido, a orientação dada para a aplicação da GDPR, modo a ser possível, assim, tanto indicar uma pessoa como DPO dentro da própria organização quanto fora dela, sendo essa pessoa externa uma pessoa natural ou uma pessoa jurídica.

Cumpre abordar, ainda, que a LGDP não expõe requisitos objetivos, relacionados à formação, capacitação técnica, a fim de autorizar a nomeação de pessoa como DPO. Todavia, de princípio, o que se pode notar é que a pessoa encarregada deve ter conhecimento suficiente relacionado à proteção de dados pessoais para desempenho de suas funções definidas na LGPD, além de, no mínimo, conhecer a própria LGPD, o que é, sem dúvida, condição *sine qua non* para que possa realizar as suas funções. Nesse sentido, ensina Bruno (2019, p. 316):

> A designação do Encarregado pelo Tratamento de Dados Pessoais deve ocorrer baseada nas qualidades profissionais do indicado, particularmente em seu conhecimento da legislação de proteção de dados, das práticas de tratamento de dados pessoais, e na sua capacidade em cumprir os requisitos da Lei Geral de Proteção de dados. Quanto mais complexas forem as atividades de tratamento de

> dados realizadas pela organização, maior deverá ser o nível de conhecimento técnico do Encarregado.

Na GDPR, o Art. 37, item 5, designa que, para a nomeação do encarregado de proteção de dados, deve-se observar “[...] suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as suas funções referidas no artigo 39.o” (UNIÃO EUROPEIA, 2016).

Conforme as orientações do Conselho Europeu (2017), o DPO deve ser escolhido com base nas suas qualidades e conhecimento, mas dentre essas qualidades deve-se observar a sua integridade e nível de ética profissional, sendo o principal a sua busca pelo cumprimento da GDPR.

E, nesse sentido, o EPD deve dar cumprimento aos elementos essenciais da GDPR, como os princípios, direitos dos titulares, proteção de dados *by design* e *by default*, registro das atividades de tratamento e segurança de tais atividades, bem como informação de incidentes de dados (CONSELHO..., 2017).

Com base na previsão da GDPR e nas orientações do Conselho Europeu, mas, primordialmente, devido aos fundamentos e princípios instituídos na LGPD, não se poderia pensar em possibilitar a nomeação de um DPO que não tivesse conhecimento especializado em proteção de dados pessoais, suficiente para fazer cumprir os preceitos da LGPD.

Inclusive, é importante notar que a LGPD não exige formação jurídica nem na área de segurança da informação, ou em qualquer outra área do conhecimento, e a GDPR, por seu turno, dispõe a necessidade de domínio do direito sobre proteção de dados, mas também não exige que o profissional tenha formação jurídica, do que se pode depreender que o conhecimento jurídico em proteção de dados é elemento essencial ao DPO, mas não que necessariamente deva ser advogado ou bacharel em Direito, podendo ser pessoa com formação em outra área do conhecimento, desde que domine o direito relativo à proteção de dados pessoais de forma suficiente.

Aqui, é importante rememorar que uma das funções do DPO, disposta no inciso III do § 2º, do Art. 41, consiste tem “orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais” e, nesse sentido, segundo Cots e Oliveira (2018, p. 220), referida previsão demonstra que o DPO “[...] não é um mero relações públicas do controlador, pois só poderá ‘orientar’ funcionários e contratados se compreender minimamente a

legislação incidente sobre a atividade, bem como os aspectos envolvidos no tratamento de dados".

A pergunta retórica que se faz é: como poderá o DPO orientar funcionários e contratados, bem como orientar boas práticas relacionadas à proteção de dados pessoais, se não possuir conhecimento suficiente sobre proteção de dados pessoais?

O DPO, nesse sentido, deve conhecer o direito relacionado à proteção de dados pessoais, mormente a LGPD, dominar as suas implicações práticas, e ter conhecimento tanto teórico quanto prático relacionado à proteção de dados, sobretudo das atividades da organização em que irá funcionar, com capacidade plena para o exercício de suas funções, com aptidão para orientar as suas funções sob os princípios da proteção de dados, fazer cumprir os direitos dos titulares e poder exercer comunicação eficiente com a ANPD.

Um DPO que não domine a matéria necessária à sua função, não terá condições técnicas de fazer cumprir a LGDP e funcionará apenas como uma figura que constará formalmente como o EPD daquela organização, sem que o espírito da Lei seja perseguido pelo desempenho efetivo de suas funções.

Nesse sentido, o Art. 41, em seu § 1º, determina que "A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador" (BRASIL 2018). Ou seja, deve-se dar publicidade ao DPO da organização, de modo a identifica-lo de forma clara, facilmente localizável, a fim de que seja contatado, o que vai ao encontro de uma das suas funções, por dever intermediar as relações com os titulares de dados e a ANPD.

A previsão da LGPD está em consonância com o que define também a GDPR, que em seu Art. 37, item 7, normatiza que "O responsável pelo tratamento ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo", ou seja, deve-se dar publicidade ao contato do DPO e, também, comunicar à Autoridade de Proteção de Dados o seu contato.

Pode-se concluir, nesse sentido, que o DPO, no sistema jurídico brasileiro, pode ser tanto uma pessoa natural quanto uma pessoa jurídica, exigindo-se, a despeito de a LGPD não o determinar expressamente, que tenha conhecimento suficiente sobre direito à proteção de dados, sob o ponto de vista teórico e prático, que possibilite o exercício de suas funções, cujo fim deve ser primar pela proteção dos dados pessoais na organização, independentemente de ter uma formação em

qualquer área do conhecimento, desde que possua os atributos suficientes a funcionar como DPO, de forma, assim, que não seja meramente um contato formal publicizado somente para dar a entender pelo cumprimento da LGDP, mas para que de fato exerça o seu papel em prol da proteção dos dados pessoais.

4.4 Conflito de interesses

Como visto, o DPO pode ser tanto uma pessoa natural quanto uma pessoa jurídica. Podendo ser uma pessoa natural, deve-se analisar a hipótese em que seja designado encarregado de proteção de dados a pessoa que já exerça alguma função em favor organização (sob qualquer forma de vínculo, como empregado, terceirizado etc), de maneira a passar a cumular suas outras funções com a de DPO. Daí que surge a possibilidade de conflito de interesses entre as duas (ou mais) funções desempenhadas, e, consoante aponta Bruno (2019, p. 316), "[...] é importante prevenir o conflito de interesses do Encarregado com outras funções que possa eventualmente exercer para a organização".

O Art. 41, § 3º da LGPD deixa a cargo da ANPD a possibilidade de complementar por meio de regulamentação a definição e as atribuições EPD, de modo que futuramente, poderá haver uma maior precisão sobre a cumulação da função de DPO, de sorte que, *prima facie*, a LGPD não se preocupou em detalhar questões como a possibilidade de cumulação de funções do DPO, nem sobre eventuais conflitos de interesses, se limitando a indicar que tanto o setor privado quanto o público devem manter um encarregado de proteção de dados.

Todavia, todas as diretrizes da LGPD e as funções do encarregado de proteção de dados, bem como a GDPR, desde já fornecem suprimentos suficientes para delinear, ainda que de forma sumária, o que constituirá ou não conflito de interesses.

Dessa forma, a própria GDPR trata a matéria expressamente em seu Art. 38, item 6: "O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento ou o subcontratante assegura que essas funções e atribuições não resultam num conflito de interesses" (UNIÃO EUROPEIA, 2016). Portanto, permite que o DPO cumule outras funções, mas condiciona essa cumulação à inexistência do conflito de interesses.

O Conselho Europeu (2017) indica em termos práticos o que constitui a inexistência desse conflito de interesses ao apontar que "[...] o EPD não pode, em

especial, exercer um cargo dentro da organização que o leve a determinar as finalidades e os meios do tratamento de dados pessoais".

E nesse mesmo sentido defende Bruno (2019, p. 317), ao lecionar que o DPO por ser o responsável por monitorar a conformidade das atividades de tratamento para que sejam realizadas em conformidade com a LGPD, de forma que, na hipótese em que ele também seja o responsável por uma atividade de tratamento, será difícil que monitore a conformidade da sua própria atividade. Outrossim, consoante aborda Mello (2019, p. 164), a LGPD deixa uma lacuna para que demais funções possam ser atribuídas ao DPO, todavia, deve-se ter por norte a preservação das atividades de tratamento sempre sob a observância da LGPD.

Outrossim, tanto cargos de gestão (como diretor executivo, de operações, financeiro, do departamento médico, de *marketing*, de recursos humanos, informático, entre outros) quanto outros de níveis inferiores podem gerar conflitos, desde que o cargo ou a função impliquem que o seu ocupante determine finalidades e meios de tratamento (CONSELHO..., 2017).

> Por exemplo, se uma empresa nomeia como Encarregado o *Compliance Officer*, e nessa função o nomeado realiza *background checks* de funcionários e terceiros, haverá nítido conflito de interesse, já que como Encarregado terá que monitorar esses *background checks* do ponto de vista da conformidade com a proteção de dados pessoais, e, como *Compliance Officer*, terá que buscar cada vez mais eficiência nessas checagens, com a coleta e tratamento cada vez maior de dados pessoais (BRUNO, 2019, p. 317).

O Conselho Europeu ainda aponta o conflito de interesses específico do DPO que é chamado para representar o agente de tratamento em processos em tribunais sobre questões de proteção de dados (CONSELHO..., 2017), o que leva a compreender que o DPO não pode atuar como representante dos interesses do agente de tratamento em processos administrativos ou judiciais – situação esta, aqui, especialmente aplicável à advocacia, sobre a qual se abordará em seção especialmente dedicada adiante.

Ainda sobre esse tema, como boas práticas, o Conselho Europeu (2017) elenca as seguintes atividades a serem promovidas pelo agente de tratamento: identificar os cargos da organização incompatíveis com a função do DPO; criar normas internas para prevenir o conflito de interesses e prever a explicação sobre o que consiste o conflito de interesses; declarar que não existe esse conflito de interesses na organização; incluir mecanismos em suas normas internas para garantir

que qualquer oferta para ocupar o cargo de DPO seja pormenorizada e precisa para evitar conflito de interesses.

Logo, o que se pode concluir é que não há qualquer vedação para que o DPO cumule funções em favor da organização, independentemente de qual seja a sua relação com essa organização, seja como empregado ou um prestador de serviços externo, desde que se observe a impossibilidade de haver conflito de interesses entre a outra (ou outras) função exercida com a função de DPO, o que se pode consubstanciar na impossibilidade de que o DPO seja, em outra função, responsável por um tratamento de dados pessoais, de maneira a definir a finalidade e o modo do tratamento de dados em favor dessa organização.

4.4.1 O DPO advogado

Questão de grande impacto prático é a discussão sobre a possibilidade de o advogado exercer a função de DPO e os eventuais conflitos de interesse daí provenientes. Assim, cabe analisar a possibilidade de o advogado atuar também, como uma segunda especialidade profissional, como DPO, a terceiros para quem não preste serviços relacionados à advocacia, bem como verificar a existência de conflito de interesses quando o advogado funcione como DPO para a mesma organização à qual exerça a advocacia.

Portanto, primeiro ponto sobre esse tema é verificar se o advogado pode atuar como DPO pura e simplesmente, partindo-se da premissa de que não exercerá qualquer atividade privativa de advogado em favor da organização em que funcione como DPO. E quanto a isso, desde já se antecipa: não há qualquer vedação.

Isso porque, em regra, não é vedado ao advogado o exercício de qualquer atividade. O Estatuto da Advocacia (EAOAB) apresenta de forma excepcional hipóteses de incompatibilidade e impedimento, e as lista, de forma taxativa, nos Arts. 28 (incompatibilidades) e 30 (impedimentos). O objetivo dessas hipóteses é: “evitar que a advocacia possa ser usada em desprestígio do interesse da coletividade mediante práticas como tráfico de influência e captação de clientela” (OABPR, 2015, p. 215).

Por essa razão, o Art. 28 o EAOAB lista as seguintes atividades que são incompatíveis com o exercício da advocacia (BRASIL, 1994):

> I - chefe do Poder Executivo e membros da Mesa do Poder Legislativo e seus substitutos legais; II - membros de órgãos do Poder Judiciário,

> do Ministério Público, dos tribunais e conselhos de contas, dos juizados especiais, da justiça de paz, juízes classistas, bem como de todos os que exerçam função de julgamento em órgãos de deliberação coletiva da administração pública direta e indireta; III - ocupantes de cargos ou funções de direção em Órgãos da Administração Pública direta ou indireta, em suas fundações e em suas empresas controladas ou concessionárias de serviço público; IV - ocupantes de cargos ou funções vinculados direta ou indiretamente a qualquer órgão do Poder Judiciário e os que exercem serviços notariais e de registro; V - ocupantes de cargos ou funções vinculados direta ou indiretamente a atividade policial de qualquer natureza; VI - militares de qualquer natureza, na ativa; VII - ocupantes de cargos ou funções que tenham competência de lançamento, arrecadação ou fiscalização de tributos e contribuições parafiscais; VIII - ocupantes de funções de direção e gerência em instituições financeiras, inclusive privadas.

Em seguida, dispõe no Art. 30 sobre as situações de impedimentos (BRASIL, 1994):

> Art. 30. São impedidos de exercer a advocacia: I - os servidores da administração direta, indireta e fundacional, contra a Fazenda Pública que os remunere ou à qual seja vinculada a entidade empregadora; II - os membros do Poder Legislativo, em seus diferentes níveis, contra ou a favor das pessoas jurídicas de direito público, empresas públicas, sociedades de economia mista, fundações públicas, entidades paraestatais ou empresas concessionárias ou permissionárias de serviço público.

A incompatibilidade determina a integral impossibilidade de exercício da advocacia, enquanto o impedimento, a impossibilidade parcial de seu exercício, consoante prescreve o Art. 27 do EAOAB (BRASIL, 1994). O que se nota, entretanto, é que o espírito da Lei tem por finalidade impossibilitar a criação de meios propícios, dentro do setor público, para a prática de ilícitos, de forma a vedar, portanto, o exercício da advocacia, total o parcialmente, para os ocupantes de certos cargos e funções.

Disso se pode depreender, com clareza, que o exercício da função de DPO não é vedado como regra. Evidentemente, se o cargo de DPO se caracterizar como um daqueles previstos no Art. 28 ou 30 o EAOAB, estará caracterizada a incompatibilidade ou o impedimento para que esse DPO exerça a advocacia.

Por exemplo, o DPO da ANPD, parece estar impedido de advogar contra a Fazenda Nacional, por força do Art. 30, I do EAOAB (BRASIL, 1994), tendo em vista que a ANPD está estruturada como um órgão da administração pública federal, e o DPO seria, assim, um servidor da administração direta.

À inexistência, por regra, de incompatibilidade ou impedimento com o exercício da função de DPO, deve-se somar o direito à liberdade de ofício, constituída na ordem jurídica como um direito fundamental, na forma do Art. 5º, inciso XIII, segundo o qual “é livre o exercício de qualquer trabalho, ofício ou profissão, atendidas as qualificações profissionais que a lei estabelecer”.

Por essas razões, dentro da ordem jurídica brasileira, está clara a possibilidade de o advogado, entendido como o inscrito na Ordem dos Advogados do Brasil, exercer as funções de DPO, pura e simplesmente, diante do direito fundamental à liberdade de ofício, e desde que o advogado não se caracterize nas hipóteses de incompatibilidade ou impedimento ao exercício da advocacia.

Ressalta-se que a análise até este momento enveredada busca responder se o advogado também pode exercer a função de DPO, sem que essa possibilidade de atuar como DPO seja analisada no caso em que o advogado presta serviços jurídicos a uma organização e nela também funcione como DPO. A conclusão que aqui, neste momento, se põe, portanto, relaciona-se à simples possibilidade de o profissional que é advogado, atuar como DPO – para empresas diante das quais não preste absolutamente nenhum serviço de natureza exclusiva da advocacia.

Segundo aspecto da análise de conflito de interesses no exercício da função de DPO sob a perspectiva do advogado, é verificar se o advogado que funciona ou funcionou como DPO para uma organização poderia prestar serviços advocatícios, sob quaisquer aspectos, como a consultoria e a promoção da defesa dos seus interesses em processos de quaisquer naturezas.

Nesse enredo, a questão parece ter objetividade para direcionar uma conclusão. Isso porque, o CEDOAB (Código de Ética e Disciplina da OAB), em seu Art. 2º, parágrafo único, estabelece, entre os deveres do advogado, no inciso VIII, alínea b), “abster-se de [...] patrocinar interesses ligados a outras atividades estranhas à advocacia, em que também atue” (CONSELHO..., 1995).

Dessa forma, é evidente que a atividade do DPO é uma atividade estranha à advocacia. A despeito de exigir conhecimento do direito à proteção de dados pessoais, envolve outros conhecimentos, ligados às práticas de tratamento de dados, de processos internos e de segurança da informação. Tanto é que a LGPD não reservou ao advogado a função de DPO, deixando aberto o exercício da função por qualquer pessoa, inclusive, podendo ser pessoa natural ou jurídica, conforme estudado outrora.

Por isso, não se verifica a possibilidade de compreender que a atividade de DPO seria reservada à classe advocatícia, de maneira que a prescrição do Art. 2º, parágrafo único, inciso VIII, alínea b) do CEDOAB, não dá margem a interpretação divergente, senão no sentido de que a função de DPO é diversa da atividade ligada à advocacia – reitera-se, a despeito de não se ignorar que o DPO deva dominar uma área específica do Direito, qual seja, a da proteção de dados pessoais.

Nesse mesmo sentido, o Conselho Geral da Ordem dos Advogados de Portugal, na conclusão do Parecer 14/99/2018-G, entendeu pela incompatibilidade do exercício da função de DPO e da advocacia no âmbito não só da defesa em processos de qualquer natureza, mas também da consultoria jurídica, em favor da organização em que a pessoa funciona ou funcionou como DPO.

Antes de concluir pela impossibilidade, o referido órgão assinalou que o exercício da função de DPO pode sim ser operado por advogado, de modo a ressaltar o conhecimento jurídico que o qualifica para tanto (CONSELHO..., 2018):

> Deve começar por se reconhecer que o Advogado estará, tecnicamente, dado o seu saber jurídico, grandemente habilitado a exercer tais funções. Verdade é que não bastarão tais conhecimentos, exigindo-se outros saberes, de natureza informática ou de tratamento de dados, por exemplo. Mas nada que o Advogado não possa adquirir e associá-los àqueles outros para bem poder desempenhar as ditas funções.

Nesse sentido o Conselho Geral da Ordem dos Advogados de Portugal reforça a conclusão anterior quanto à juridicidade de o advogado poder exercer a função de DPO, mormente, como ressaltado, pelo conhecimento jurídico que lhe é intrínseco, de modo que a este caberá adquirir os demais conhecimentos fundamentais à função de encarregado de proteção de dados.

Entretanto, ao abordar a possibilidade de exercer, de forma cumulada, a advocacia e a função de EPD em favor de uma mesma organização, a conclusão é no sentido da impossibilidade, sobretudo porque a função de DPO será de fiscalizar a organização, o que se mostraria incompatível com a defesa dos interesses do mesmo cliente (CONSELHO..., 2018):

> Na verdade, o advogado deve considerar-se impedido de praticar atos profissionais para clientes onde desempenhe ou tenha desempenhado funções, como as próprias do DPO, cujo exercício pode suscitar, em concreto, uma incompatibilidade, se aqueles atos entrarem em conflito, como é seguro, com as regras deontológicas que regulam o exercício da atividade da advocacia.
> A advocacia deve ser exercida de forma isenta e independente. Isso não significa que o advogado deva ser imparcial (isso deve ser o juiz).

> O advogado diria que, por definição, é parcial. Sendo assim, parece evidente que relativamente a um determinado cliente, tendo a obrigação de, como DPO, o fiscalizar – com tudo o que isso implica regulamentarmente – deontologicamente não tem condições para de lhe prestar a sua atividade como advogado, no âmbito do mandato forense e da consulta jurídica.
> [...]
> Nos termos do disposto no artigo 83.º, 1, 2 e 6, do Estatuto da Ordem dos Advogados, os advogados estão impedidos de exercer a advocacia e, assim, impedidos de exercer o mandato forense ou a consulta jurídica, para entidades para quem exerçam, ou tenham exercido as funções de Encarregado de Proteção de Dados.

Vê-se, portanto, que pelas razões de o advogado dever exercer a advocacia de forma isenta e independente, e, inclusive, de forma parcial, ao passo que na função de encarregado de proteção de dados deve atuar de forma a fiscalizar a organização e cumprir seus deveres atribuídos a esta função, o Conselho Geral da Ordem dos Advogados de Portugal vedou o exercício da advocacia, consubstanciada tanto no mandato forense quanto na consultoria jurídica, em favor de entidade a quem o advogado atue ou tenha atuado como DPO.

Outrossim, o Conselho Europeu (2017) orienta, exemplificativamente, a existência de conflito de interesses na situação em que o DPO realiza a defesa da organização: “pode igualmente surgir um conflito de interesses se, por exemplo, um EPD externo for chamado a representar o responsável pelo tratamento ou o subcontratante perante os tribunais no âmbito de processos respeitantes a questões de proteção de dados”.

O que se depreende, assim, é que o advogado, na atividade de consultoria e de patrocínio de demandas administrativas e judiciais, atua de forma parcial, na defesa dos interesses do seu cliente. Conforme exemplifica o Art. 2º, §2º, do EAOAB, “No processo judicial, o advogado contribui, na postulação de decisão favorável ao seu constituinte, ao convencimento do julgador, e seus atos constituem múnus público” (BRASIL, 1994).

É papel do advogado, portanto, exercer o seu ofício para obter resultado favorável ao seu cliente, a envidar esforços para convencer a autoridade e, assim, lograr êxito em decisão que melhor atenda aos interesses da parte que patrocina, ou seja, é sujeito que atua de maneira parcial, em favor do representado.

Outrossim, exteriormente à atividade forense, ao atuar no interesse do cliente, o papel do advogado consiste em apresentar as melhores soluções jurídicas em favor da organização, de forma a agir dentro da legalidade, evidentemente, todavia,

trabalhar os aspectos jurídicos do ponto de vista que mais favoreça a parte interessada que é sua contratante, inclusive valendo-se de, na existência de entendimentos divergentes sobre certas matérias, esforços para subsumir a situação fática do consultante de modo a lhe trazer a mais benéfica situação jurídica.

De outro lado, ao se analisar as funções do DPO, entretanto, dentro do contexto de proteção idealizado pela LGPD, seu papel é funcionar em favor do cumprimento das disposições da LGPD, como esclarecem as atividades dispostas no Art. 41, § 2º da Lei.

O EPD, portanto, deve atuar de forma a se comunicar com os titulares de dados, ou intermediar essa comunicação, de modo a prestar esclarecimentos e adotar providências em favor dos titulares de dados (inciso I). Também, deve servir de canal entre o agente de tratamento e a ANPD, a adotar providências por esta solicitadas (inciso II). E, com maior amplitude de aplicação, deve orientar funcionados e contratados sobre as práticas a sem adotadas sob as previsões da LGPD (inciso III).

E a observância da LGPD, implica, portanto, o dever de atuar para o seu cumprimento nas atividades de tratamento de dados pessoais, com o objetivo de que estas sejam operadas sob os ditames dos direitos de proteção de dados pessoais, de maneira a cumprir os fundamentos da LGPD, a sua principiologia, enfim, todas as suas normas, dentre elas, o objetivo da Lei. Conforme pondera Mello (2019, p. 164) sobre a função do DPO, “[...] seu papel é de preservar a atividade de tratamento de dados em consonância com os princípios fundamentais da Lei”.

Lembre-se, nesse sentido, que o objetivo da LGPD é, conforme projeta seu Art. 1º, *caput*, “[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018). E isso quer dizer que a sua concepção designa que todas as suas normas instituídas têm por fim a proteção da pessoa natural.

E, nesse sentido, todo o regime jurídico idealizado na LGPD tem por condão a proteção de dados pessoais, é dizer, busca assegurar a proteção das pessoas naturais, no contexto da sociedade da informação ora estabelecido, no qual os dados pessoais são objeto de operações de tratamento constantemente, potencializadas pelo uso da internet e dos ambientes digitais, em que os dados se tornaram o bem de maior valor agregado – na economia da informação, é a informação o seu valor central.

Assim – além da própria previsão do CEDOAB, que veda o patrocínio de interesses ligados a outras atividades diversas da advocacia em que o advogado também atua, além da mesma orientação do Conselho Geral da Ordem dos Advogados de Portugal, tanto no âmbito da consultoria quanto no da atividade forense, e além de o próprio Conselho Europeu orientar a incompatibilidade entre a função de DPO e a defesa de interesses em processos relacionados a proteção de dados pessoais em favor da mesma organização –, o conflito de interesses entre o exercício da advocacia (de forma consultiva ou na atuação em processos de quaisquer naturezas), tanto quanto à matéria de proteção de dados pessoais quanto relacionados a quaisquer outras matérias, e o exercício da função de DPO em favor de um mesmo cliente, é perceptível pela própria concepção das funções.

Isso porque, o encarregado de proteção de dados, a despeito de exercer sua atividade em favor de uma organização, o faz inserido no contexto da LGPD, cuja aplicação tem o dever de orientar, ou seja, ele exerce a função de DPO em prol da organização para o fim de que as atividades de tratamento operadas respeitem todo o sistema jurídico relacionado à proteção de dados pessoais, cujo objetivo estampado logo no Art. 1º da LGPD é “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018), enquanto o advogado, ao atuar em consulta ou em patrocínio de processos, sejam judiciais ou administrativos o faz em favor do seu cliente, no interesse do seu contratante.

O conflito de interesses é nítido: o DPO deve buscar a proteção dos titulares de dados, ou seja, atua como encarregado do tratamento de dados para a organização, mas de maneira a buscar que as operações de tratamento ocorram sob os ditames da LGPD, no interesse, logo, dos titulares de dados; ao advogado, na outra mão, cabe a defesa e orientação dos aspectos jurídicos do ponto de vista dos interesses do seu cliente, seu contratante.

Desse modo, fica claro que ao profissional que exerça a advocacia e, ao mesmo tempo, a função de DPO, deverá escolher diante de uma organização qual serviço lhe irá prestar: serviços advocatícios ou de encarregado de proteção de dados, não podendo cumular ambas as funções, nem contemporaneamente, nem posteriormente.

Isso porque, permitir que esses serviços se cumulem, ou mesmo que, posteriormente ao exercício da função de DPO, já cessado, se exerça a advocacia,

implicará em admitir que esse profissional releve ou os interesses dos titulares de dados ou os interesses do seu cliente contratante, o que, nesse sentido, seria antijurídico, por ser potencialmente contrário ou ao espírito da LGPD – cujo objetivo é a proteção do titular de dados – ou ao espírito do papel da advocacia – exercida de maneira parcial em favor dos interesses do cliente, jurisdicionado.

Em suma, portanto, em relação ao conflito de interesses entre o exercício da advocacia e, cumulativamente, a função de DPO, pode-se analisar duas hipóteses. A primeira, a possibilidade de o advogado exercer também uma outra especialidade profissional, a função de DPO, o que é lícito, portanto. A segunda, o nítido conflito de interesses entre o advogado que presta serviços a uma organização também funcionar como DPO em favor desta, por serem característicos os interesses divergentes entre a proteção que busca a LGPD aos titulares de dados, à qual deve zelar o DPO ao funcionar como encarregado do tratamento de dados em uma organização, e o exercício da advocacia, tanto na consultoria quanto no mandato forense, nos quais o advogado envida todos os seus esforços para atender aos interesses do seu cliente contratante.

Logo, o advogado é livre para atuar também como DPO, desde que não existam incompatibilidades ou impedimentos nos termos do EAOAB. Entretanto, ao se analisar a cumulação de prestação de serviços de advocacia e de DPO em favor de uma mesma organização, haverá inafastável conflito de interesses porque o interesse perseguido pelo DPO é o do titular de dados, enquanto o interesse perseguido pelo advogado é o do seu cliente, que lhe contrata para promover a sua defesa em procedimentos judiciais ou administrativos, e, assim, defendê-lo, em seus interesses, ou para lhe apresentar as melhores soluções jurídicas, que lhe tragam benefícios, dentro da licitude, inclusive, diante de situações jurídicas em que haja entendimentos variados, conclusão esta, aliás, que está em consonância com a paradigmática decisão da Ordem dos Advogados de Portugal, conforme parecer 14/99/2018-G (CONSELHO..., 2018), que concluiu pela incompatibilidade do exercício da função de DPO e da advocacia para uma mesma entidade, no âmbito não só da defesa em processos de qualquer natureza, mas também da consultoria jurídica, em favor da organização em que a pessoa funciona ou funcionou como DPO.

Assim, trazendo-se a mesma conclusão adotada pela Ordem dos Advogados de Portugal, que está em consonância, frisa-se, com o ordenamento jurídico brasileiro, ao advogado é lícito atuar como DPO, todavia, não poderá prestar serviços jurídicos

à entidade para quem atue ou tenha atuado como encarregado de proteção de dados. Em termos práticos, o profissional advogado, se se puser diante de tal circunstância, deverá escolher entre prestar serviços privativos da advocacia ou o serviço de DPO à organização.

4.5 Obrigatoriedade do DPO, o operador e o controlador, as diferentes formatações empresariais e o compartilhamento do DPO externo

A Lei obriga que todas as organizações privadas e entes públicos, tenham DPO, por menor que seja a sua estrutura, desde que se enquadrem no conceito de operador de dados. Conforme dispõe o *caput* do Art. 41 da LGPD: "O controlador deverá indicar encarregado pelo tratamento de dados pessoais" (BRASIL, 2018). Pelo que está definido, até então, na LGPD, o controlador deve nomear um encarregado de proteção de dados pessoais.

Acontece que o § 3º do Art. 41, dispõe que (BRASIL, 2018):

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

Ou seja, a LGPD deixou a cargo da ANPD, ao autorizá-lo expressamente, que de acordo com a natureza, o porte ou volume de operações de tratamento de dados, em normas complementares, poderá ser dispensada a indicação do DPO. Trata-se, portanto, de disposição em que a Lei reserva à ANPD a faculdade de afastar a obrigatoriedade posta como regra no *caput* do Art. 41.

Sobre a possibilidade de afastar a obrigatoriedade de indicação do DPO, conforme a natureza, porte ou volume de dados tratados, Cots e Oliveira (2018, p. 219) defendem que "como o § 3º utiliza o verbo 'poderá', não gerando a obrigatoriedade por parte da autoridade nacional, a nosso ver, até que a autoridade seja criada e retire a necessidade de indicação, todos os controladores deverão indicar seus encarregados".

Nesse sentido, de fato, não há conclusão a se extrair da redação clara do Art. 41, senão no sentido de que, até que a ANPD afaste a obrigatoriedade de nomeação do DPO pelo controlador, deve este fazê-lo.

Por outro lado, ao operador não foi imposta a obrigatoriedade de nomeação de um DPO, o que não impede, todavia, que o faça. Aliás, a nomeação de um DPO

seja por um operador, seja por um controlador que eventualmente venha a ser dispensado da obrigatoriedade por norma da ANPD, constitui atitude louvável do ponto de vista da proteção instituída pela LGPD. Entretanto, “[...] o entendimento é de que tudo quanto aplicável em relação ao Encarregado obrigatório também será aplicável ao Encarregado nomeado em base voluntária” (BRUNO, 2019, p. 315). Bruno (2019, p. 315) ainda indica que:

> [...] o fato da organização não designar um Encarregado pelo Tratametno de Dados Pessoais, por entender desnecessária a função, não a desobriga do cumprimento das obrigações previstas na Lei Geral de Proteção de Dados, muito menos eximirá a organização de alocar seu pessoal ou consultores externos em assuntos relacionados à proteção de dados pessoais [...]

Veja-se, assim, que a organização dispensada da indicação do DPO pode indica-lo, voluntariamente, ocasião em que, entretanto, deverão ser observados todos os aspectos deontológicos da atividade do encarregado de proteção de dados. E, na hipótese de sua dispensa, de qualquer modo, a atividade deverá observar os demais preceitos da LGPD e de proteção de dados pessoais dispostos em quaisquer normas incidentes, porquanto a ausência de obrigatoriedade de indicação do DPO não exime a atividade de promover a proteção dos dados pessoais – até porque a LGPD não o possibilita em qualquer disposição àqueles desobrigados da indicação do encarregado do tratamento de dados.

Na GDPR a obrigatoriedade de indicação o encarregado de proteção de dados está vinculada a critérios objetivos, diversa do critério subjetivo adotado pela LGPD. Assim, são hipóteses obrigatórias de indicação do EPD na GDPR (UNIÃO EUROPEIA, 2016):

> a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;
> b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
> c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.o e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o.

Para melhor elucidação, as categorias de dados especiais mencionadas no item “c)”, diz respeito aos correspondentes dados sensíveis na LGPD:

> [...] origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Pode-se observar, nesse contexto, que a GDPR atribuiu a obrigatoriedade de indicação do DPO conforme critérios objetivos, relacionados ou ao agente de tratamento ou à própria atividade de tratamento de dados pessoais, enquanto, de outro lado, a LGDP optou por, em regra, atribuir a obrigatoriedade com base no critério objetivo da pessoa do controlador, e resvalou a indicação de excepcionais critérios objetivos (conforme a natureza, porte e volume de atividades de tratamento de dados) a norma a ser editada pela ANPD.

Logo, a indicação do DPO é obrigatória para o controlador, por expressa determinação do Art. 41 da LGPD – a ser este o critério objetivo adotado no ordenamento jurídico brasileiro, diverso das situações objetivas, relacionadas às atividades dos agentes ou às atividades de tratamento, adotado pela GDPR.

Até que haja determinação em sentido diverso, a indicação do encarregado é obrigatória para todo e qualquer controlador, o que poderá ser reformatado pela ANPD, à qual foi atribuída a faculdade de promover a dispensa de indicação do DPO, conforme a natureza, porte e volume de tratamento de dados – situação em que a ANPD poderá, assim, utilizar critérios objetivos, semelhantes aos da GDPR, para autorizar a dispensa do DPO.

Por fim, na hipótese de desobrigação da indicação do DPO: caso seja indicado de forma voluntária, o regime jurídico aplicado ao DPO de designação obrigatória deve ser igualmente observado; de qualquer modo, todas as normas relativas à proteção de dados pessoais, presentes na LGPD ou não, são de observância imperativa.

No que tange à possibilidade de dispensa do DPO, reflexões devem ser fomentadas tendo em vista a busca pela preservação da igualdade em seu sentido material no âmbito das atividades econômicas. Para isso, utiliza-se um dos critérios mencionados para a potencial dispensa do DPO, definidos no § 3º do Art. 41 da LGPD: o porte da atividade.

Dessa forma, a análise do porte das atividades é essencial a fim de não onerar e fazer pairar sobre atividades econômicas diminutas o ônus da indicação de um DPO que pode comprometer o seu próprio desenvolvimento. Rememore-se que um dos fundamentos da LGPD, conforme Art. 2º, inciso V, é o desenvolvimento econômico

(BRASIL, 2018), de modo que deve haver a compatibilização entre o novo regime de proteção de dados pessoais de forma a assegurar, ao mesmo tempo, que não haverá óbices ao desenvolvimento das atividades econômicas.

Aliás, é para esse objetivo que a CF, Art. 170, estabelece como um dos princípios da ordem econômica, em seu inciso IX, o "tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País" (BRASIL, 1988). Sobre esse tratamento diferenciado às atividades econômicas de pequeno porte, ponderam Bastos e Martins (2000, p. 36-37):

> [...] compreensível que se tenha querido dar tratamento favorecido a essas empresas sobretudo quando se leva em conta que não é justo impor-se-lhes a mesma quantidade de ônus burocrático que descarregado em cima das macroempresas, que evidentemente dispõem de recursos em muito maior quantidade para poder enfrentar esta carga burocrática. O mesmo se pode dizer relativamente aos tributos".

Também sobre o tratamento diferenciado de tais atividades, ensina Cretella Júnior (1993, p. 4.162):

> [...] preocupado com a ordem econômica, fundada na valorização do trabalho humano e na livre-iniciativa, assegurando a existência digna, o legislador constituinte, conforme os ditames da justiça social, erigiu, como princípio informativo, o tratamento favorecido para as empresas de capital nacional de pequeno porte (art. 170, Iv), favorecendo-as mediante tratamento jurídico, diferenciado, visando incentivá-las, mediante a simplificação de suas obrigações (a) administrativas, (b) tributárias, (c) previdenciárias, (d) creditícias ou (e) pela eliminação ou (f) pela redução destas obrigações, por meio de lei.

Portanto, a Constituição Federal buscou estabelecer um regime diferenciado para as empresas de pequeno porte, a fim de desonerá-las das mesmas obrigações que recaem sobre grandes agentes econômicos, de maneira a simplificar suas obrigações, eliminando-as, ou reduzindo-as, isso para fomentar, ao fim, o exercício dessas atividades e, em última análise, o desenvolvimento da economia nacional.

Nesse contexto, não se poderia eximir o regime de proteção de dados pessoais instituído pela LGPD, cuja complexidade atribuível às grandes empresas não pode recair, sob os mesmos ditames – buscando-se não ensejar prejuízo ao titular de dados pessoais simultaneamente –, às pequenas organizações, que merecem, por força da Constituição Federal, Art. 170, inciso IX, tratamento jurídico diferenciado.

A fim de apenas fomentar a complexidade da questão – e jamais com a pretensão de resolvê-la de maneira definitiva – se estabelece critérios exemplificativos

para classificação de grandes, médias e pequenas organizações, considerando-se características estruturantes para análise da possibilidade do ponto de vista de recursos financeiros para indicação de um encarregado de proteção de dados pessoais.

O critério que se sugere, exemplificativamente, para delinear o que são grandes, médias e pequenas organizações é aqui definido da seguinte forma: a grande organização é aquela em que há relevância econômica e clara subdivisão em setores, multifuncionais, na qual é possível incorporar um comitê multiprofissional para tratar especialmente do tema de privacidade e proteção de dados pessoais; a média organização é aquela em que não é possível atribuir a um grupo específico de colaboradores essa atuação, de modo a ser possível designar apenas um DPO, que irá atuar em colaboração com outros profissionais, como o corpo jurídico, interno ou externo, ou ainda em que o DPO cumula essa função com outras funções dentro da organização; a pequena organização seria aquela em que não existe uma clara divisão de funções, na qual existe um enxuto número de colaboradores que desempenham diversas funções, como quando se verifica que uma só pessoa é diretora das operações, mas também realiza vendas, é responsável com compras junto a fornecedores, realiza atendimento direto ao cliente, etc.

Sob os diferentes cenários das grandes, médias e pequenas organizações, as exigências relacionadas ao DPO devem também ser diversas. Ou seria possível manter a exigência de uma pequena organização, em que a atividade tem pouca relevância econômica, na qual o seu diretor se confunde com a pessoa que também atende o cliente e que realiza a limpeza física do estabelecimento, a fim de que mantenha um DPO, e, ao mesmo tempo, observar o fundamento do desenvolvimento econômico, previsto no Art. 2º, inciso V, da LGPD, e ainda compatibilizar essa exigência com o tratamento diferenciado instituído pela CF, Art. 170, inciso IX?

Pelo que já ponderado, a resposta parece ser negativa. Não foi à toa, inclusive, que a própria LGPD instituiu a possibilidade de a ANPD, conforme autorização expressa do Art. 41, § 3º, promover a dispensa de indicação do DPO. E, assim como as diferenças entre os portes das atividades, a natureza e o volume de dados tratados devem ser determinantes à flexibilização ou à dispensa da indicação.

Como sugere Mello (2019, p. 165), “[...] não seria razoável esperar que o João das Couves, dono de um mercadinho de bairro, que faz um controle mínimo de dados, instituísse um encarregado pelo tratamento de dados”.

Logo, caberá à ANPD promover o quanto antes a edição de normas regulamentadoras, para compatibilizar a indicação do DPO com as diversas formatações de atividades empresárias, a fim de estabelecer tratamento equitativo conforme a natureza, porte e volume de operações de tratamento de dados, com vistas a compatibilizar a exigência do DPO com o desenvolvimento econômico que a própria LGPD resguarda e com o tratamento diferenciado garantido às atividades empresariais de pequeno porte que a CF assegura.

Por fim, quanto à indicação do DPO, é pertinente verificar a possibilidade de compartilhamento de um encarregado de dados que atue externamente, de forma a atender diversos clientes, sendo o exercício da função de DPO o seu ofício, prestado simultaneamente a diversas organizações.

Na esteira do abordado outrora, a LGPD, em sua redação atual, permite que tanto pessoas naturais quanto pessoas jurídicas possam desempenhar o papel de encarregado de proteção de dados, o que segue, nesse sentido, a orientação dada para a aplicação da GDPR, modo a ser possível, assim, tanto indicar uma pessoa como DPO dentro da própria organização quanto fora dela, sendo essa pessoa externa uma pessoa natural ou uma pessoa jurídica.

O encarregado de proteção de dados externo, terceirizado, se tornou uma figura popularmente conhecida como DPO *as a service*, o que significa, portanto, o DPO como um serviço, a constituir um serviço comum na Europa, em que empresas especializadas se propõem a exercer as funções de DPO em prol da organização.

Por seu turno, a LGPD, nem em relação às pessoas naturais nem em relação às pessoas jurídicas, promoveu qualquer vedação à prestação dos serviços relativos à função de DPO de forma compartilhada, o que significa dizer que uma pessoa natural ou uma pessoa jurídica não está proibida pela LGPD de atuar como DPO de forma simultânea a diversos agentes de tratamento.

Aliás, como já consignado, o Conselho Europeu (2017), em suas orientações, aponta as vantagens da existência de uma organização especializada em executar as funções de encarregado de proteção de dados: “Simultaneamente, as competências e os pontos fortes individuais podem ser combinados de modo que várias pessoas, trabalhando em equipa, possam servir os seus clientes de forma mais eficiente”.

Não obstante, deve-se observar que a possibilidade regulamentar da ANPD não admite que esta promova qualquer restrição nesse sentido, tendo em vista que o § 3º do Art. 41 se concebeu para o fim de mitigar a obrigação relativa à indicação do

DPO, de modo a não parecer permitir que a ANPD endureça a obrigatoriedade, mas que tão somente tenha a faculdade de flexibilizá-la, ao designar expressamente sobre a possibilidade de dispensa mas, de outro lado, não ponderar qualquer possibilidade de alargar a obrigatoriedade já instituída pelo *caput* do Art. 41, repisa-se: “A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação [...]” (BRASIL, 2018). Fosse a vontade da LGPD admitir o endurecimento da indicação do DPO, teria resvalado tal possibilidade para regulamentação da ANPD.

Dessa forma, não há por que se depreender pela ilegalidade do compartilhamento de encarregados de proteção de dados, sejam pessoas naturais ou pessoas jurídicas, que prestem referido serviço de forma terceirizada e especializada.

Aliás, cumpre apontar que a própria GDPR, em seu Art. 37, item 1, dispõe que: “Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que haja um encarregado da proteção de dados que seja facilmente acessível a partir de cada estabelecimento”. Conforme leciona Saldanha (2018, p. 116) especificamente sobre referido dispositivo da GDPR, “O objetivo é libertar as organizações de custos acrescidos, desde que elas sejam responsáveis na escolha e na determinação da visibilidade e disponibilidade do DPO”.

Veja-se que o que ressalta a GDPR, e que deve ser levado em consideração, é a fácil acessibilidade a partir de cada estabelecimento. Dessa forma, o DPO externo, compartilhado para várias organizações, deve ser facilmente acessível a partir das referidas atividades, sem que haja prejuízo em razão da circunstância do compartilhamento, para o regular exercício das suas funções.

Como ponderam as orientações do Conselho Europeu (2017), “a fim de assegurar que o EPD, seja interno seja externo, esteja acessível, é importante garantir a disponibilidade dos seus contactos, em conformidade com os requisitos do RGPD”. No mesmo sentido, portanto, sob a luz da LGPD, deve-se publicizar o contato do DPO, de maneira regular, de sorte a atender a disposição do Art. 41, § 1º, da LGPD.

Nesse sentido, Bruno (2019, p. 318) corrobora a presente conclusão ao consignar que: “[...] a legislação não veda a nomeação de um Encarregado pelo Tratamento de Dados Pessoais para mais de uma empresa, de modo que um único Encarregado pode atender mais de uma companhia”.

Ora, ante a ausência de qualquer vedação à contratação do DPO externo, que preste esse serviço de forma especializada, pode-se depreender pela possibilidade

de compartilhamento do DPO, evidentemente, desde que tal circunstância não cause qualquer imbróglio ao eficiente desenvolvimento da função. Entretanto, mais uma vez, como orientou o Conselho Europeu (2017), a atividade especializada, na verdade, tem o condão de conferir maior vantagem, dada a maior eficiência que dela pode decorrer.

Pelo exposto, fica claro que o DPO pode ser uma consultoria externa, especializada no exercício das funções de encarregado do tratamento de dados pessoais, desde que seja facilmente acessível, regularmente, conforme determina o Art. 41, § 1º da LGPD, e desde que às funções não haja qualquer prejuízo frente à circunstância de compartilhamento entre os vários agentes de tratamento que podem contratar a consultoria especializada, seja de pessoa natural, seja de pessoa jurídica.

4.6 Autonomia da atuação e documentação dos atos

A função do DPO é assegurar que o tratamento de dados seja promovido sob os ditames da LGPD. Nesse sentido, pretende-se responder, neste momento, quais as perspectivas de autonomia para atuação do encarregado de proteção de dados, e, nesse contexto, avaliar a documentação dos seus atos no exercício da sua função.

A LGPD, no § 3º do Art. 41, confere à ANPD a atribuição de dar melhor especificidade à definição e às atribuições do DPO (BRASIL, 2018), e, assim, não explicita com literalidade sobre a sua autonomia. Entretanto, do espírito da LGPD, em consonância com a inspiradora deste diploma, GDPR, não se pode concluir algo que não seja a autonomia do DPO para atuar em prol do tratamento de dados pessoais sob a égide do objeto da LGPD, em favor dos titulares de dados, a fim de que lhes sejam assegurados todos os direitos estabelecidos no sistema de proteção de dados pessoais.

O DPO, conforme *caput* do Art. 41 da LGPD, é “encarregado pelo tratamento de dados pessoais” (BRASIL, 2018). Ao se analisar as suas funções no § 2º do mesmo dispositivo, este deve atuar como um meio de comunicação com os titulares de dados, prestando-lhes esclarecimentos e adotando providências, e deve, também, agir como intermediário entre o agente de tratamento e a ANPD, de modo a, também, adotar providências por esta solicitadas, e, ainda, deve orientar tanto funcionários como contratados do agente de tratamento sobre as práticas de tratamento em relação à proteção de dados pessoais, não se podendo admitir, jamais, que a LGPD lhe tenha imposto essa orientação senão sob o sistema de proteção conferido pela LGPD, evidentemente (BRASIL, 2018).

É seu papel, portanto, em relação aos próprios titulares de dados, à ANPD, e em relação aos colaboradores da organização, agir e orientar a fim de que as normas de proteção de dados pessoais sejam regularmente aplicadas, sendo encarregado pelo tratamento de dados pessoais, de forma a garantir que o tratamento seja operado de forma lícita, sob a normatização da LGPD e eventuais normas esparsas sobre proteção de dados pessoais aplicáveis à atividade empresária em que funciona. E, por essa razão, deve primar pela observância do próprio objeto da LGPD, que em seu Art. 1º, no *caput*, enuncia o objetivo de proteger os direitos de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

A GDPR auxilia, com alto grau de clareza, a compreensão sobre a autonomia do DPO para atuar em prol do tratamento dos dados pessoais com o objetivo de assegurar os direitos dos titulares. Os itens 1 a 3 do Artigo 38.º da GDPR, que abordam a "posição do encarregado da proteção de dados", nesse sentido, atribuem de modo explícito a impossibilidade de ingerência do agente de tratamento diante da atuação do EPD.

Conforme designa o Art. 38.º, item 1, da GDPR "O responsável pelo tratamento e o subcontratante asseguram que o encarregado da proteção de dados seja envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais" (UNIÃO EUROPEIA, 2016).

Em seguida, a GDPR assegura, no item 2 do Art. 38.º:

> O responsável pelo tratamento e o subcontratante apoia o encarregado da proteção de dados no exercício das funções a que se refere o artigo 39.o, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento (UNIÃO EUROPEIA, 2016).

Visa-se, assim, que ao DPO não seja suprimido qualquer conhecimento sobre as atividades de tratamento desempenhadas pela organização. Envolvê-lo, adequadamente, e sem demora, dando-lhe acesso sobre as questões relativas ao tratamento de dados pessoais, importa, nesse sentido, dar-lhe ciência do que o agente de tratamento está a operar quanto ao tratamento de dados pessoais. Sendo encarregado por este, portanto, incumbe-lhe ter plena clareza e envolvimento em relação ao que quer que esteja o agente de tratamento e promover quanto a dados pessoais.

É claro, assim, e no mesmo sentido do espírito da LGPD, que ao DPO – como responsável pelo tratamento dos dados pessoais, por lidar com os titulares de dados, com a ANPD, e por ser responsável pela atuação de funcionários e contratados em relação a proteção de dados pessoais sob a égide da LGPD – se deve garantir acesso a todas as atividades da organização que envolvam, de qualquer forma, tratamento de dados pessoais.

É interessante, ainda, que a GDPR expõe que deve o EPD não só ter conhecimento, acesso, ou saber o que está a organização a realizar quanto à matéria de dados pessoais. Mas garante-lhe mais: "envolvimento", conforme item 1 do Art. 38.º. Isso quer dizer, assim, que ao DPO não se deve apenas dar ciência sobre todas as questões de dados pessoais, mas também permitir-lhe sobre elas exercer as suas funções, orientar, para que o tratamento de dados pessoais seja operado sob a licitude, o que, sem dúvida, está em consonância com a sua função na LGPD: se deve orientar os funcionários e colaboradores, certo é que deve se envolver em todas as atividades de tratamento de dados pessoais a fim de que possa fazê-lo satisfatoriamente.

Por sua vez, o item 3 do Art. 38.º, de importante relevância para a compreensão da autonomia da atuação do DPO, prescreve que:

> O responsável pelo tratamento e o subcontratante asseguram que da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções. O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante (UNIÃO EUROPEIA, 2016).

Em consonância com esse dispositivo, está o considerando 97 da GDPR, que sobre o DPO, pondera que "sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência" (UNIÃO EUROPEIA, 2016).

Ou seja, nos termos da GDPR, o DPO deve agir de forma autônoma, e não sob as instruções do agente de tratamento, não pode ser destituído nem penalizado por exercer as suas funções, e tem acesso direto, sem passar por intermediários da organização, a qualquer de seus colaboradores, do mais baixo ao mais alto cargo, e, ainda, como informa o considerando indicado, deve estar em condições de desempenhar as suas funções e atribuições de maneira independente.

O DPO não receber instruções é de alto significado, e vai ao encontro do considerando 97, no sentido de que deve atuar para garantir o direito à proteção de dados pessoais, cujo objetivo último é assegurar todos os direitos aos seus titulares, de maneira que o agente de tratamento não pode direcionar o seu trabalho, cuja direção não pode ser outra senão garantir os direitos dos titulares de dados, para a qual foi concebida a GDPR.

E, nesse mesmo sentido, a não penalização e destituição pelo exercício de suas funções, somada à possibilidade de se dirigir diretamente a qualquer pessoa da organização, sem que haja intermediários entre o EPD e quaisquer colaboradores, reforçam a sua autonomia para agir em prol da proteção dos dados pessoais, sem obstáculos para garantir os direitos dos titulares de dados.

Como orienta o Conselho Europeu (2017), sobre o item 3: “estabelece determinadas garantias básicas no sentido de ajudar a assegurar que os EPD tenham condições para executar as suas tarefas com suficiente grau de autonomia no seio da sua organização”. Assim, o próprio Conselho Europeu, de forma expressa, atribui que ao DPO deve ser assegurada a autonomia, por ser este o objetivo da GDPR. Ainda, para o Conselho Europeu (2017):

> Significa isto que os EPD, no exercício das suas funções ao abrigo do artigo 39.º, não devem receber instruções quanto à forma de tratar uma questão, por exemplo quanto ao resultado que deve ser obtido, à forma de investigar uma queixa ou à necessidade de consultar a autoridade de controlo. Além disso, não devem receber instruções no sentido de adotarem determinada perspetiva sobre uma questão relacionada com as normas de proteção de dados, por exemplo determinada interpretação da legislação.

Ao se trazer tão perspectiva da GDPR às funções atribuídas ao DPO pela LGPD, é de se concluir que o mesmo nível de autonomia deve-lhe ser assegurado no sistema jurídico de proteção de dados pessoais no Brasil. Relembre-se que o DPO deve, frente aos titulares de dados, à ANPD, e aos colaboradores da organização, agir e orientar a fim de que as normas de proteção de dados pessoais sejam regularmente aplicadas, sendo encarregado pelo tratamento de dados pessoais, de forma a garantir que o tratamento seja operado de forma lícita, sob a normatização da LGPD e eventuais normas esparsas sobre proteção de dados pessoais aplicáveis à atividade empresária em que funciona. E, dessa maneira, deve primar pela observância do próprio objeto da LGPD, que em seu Art. 1º, no *caput*, enuncia o objetivo de proteger

os direitos de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Não se pode conceber, portanto, que o encarregado de proteção de dados no Brasil possa exercer as suas funções sem que tenha conhecimento, acesso e envolvimento em todas as atividades de tratamento de dados pessoais da organização, ou que seja punido ou destituído por buscar cumprir as suas funções na exatidão do proposto pela LGPD, ou exercer suas funções mediante imposição de orientações do agente de tratamento ou, ainda, sem que possa se direcionar a qualquer dos colaboradores da organização.

Logo, em consonância com as funções atribuídas pela LGPD, e sob o paradigma da GDPR, o DPO deve atuar com autonomia, sem ingerências do agente de tratamento que lhe indica à função, tendo acesso e envolvimento em todas as atividades de tratamento da organização em que funciona, com vistas a promover a observância do sistema de proteção de dados pessoais instituído pela LGPD, com o objetivo máximo e final de assegurar aos titulares de dados todos os seus direitos.

Sob o prisma da então concluída autonomia do DPO, deve-se analisar o dever de cumprimento do princípio prestação de contas, elencado no Art. 6º da LGPD, inciso X: “responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (BRASIL, 2018).

A autonomia conferida ao DPO, entretanto, não pode ser confundida com a tomada de decisão sobre o tratamento de dados pessoais pela organização. Como já está claro neste momento, a sua função é atuar para que a LGPD seja aplicada, agindo como um orientador dos seus preceitos, o que, todavia, não importará na tomada de decisão sobre finalidades e meios de tratamento dos dados pessoais, decisões que incumbirão ao próprio agente de tratamento. Como orienta o Conselho Europeu (2017):

> A autonomia dos EPD não implica, contudo, que lhes sejam conferidos poderes decisórios que extravasem as suas funções em conformidade com o artigo 39.º.
> O responsável pelo tratamento ou o subcontratante permanece responsável pelo cumprimento das normas de proteção de dados e deve poder comprovar esse cumprimento. Se o responsável pelo tratamento ou o subcontratante tomar decisões incompatíveis com o RGPD e o parecer do EPD, deve ser dada a possibilidade ao EPD de

> transmitir de forma clara o seu parecer divergente ao mais alto nível da direção e a quem tomou as decisões.

Assim, ao DPO cabe agir para que as decisões sejam tomadas em consonância com o sistema de proteção de dados pessoais, de forma a orientar o agente de tratamento que lhe contrata a fim de que aja sob tais ditames, de modo que seu contratante estará livre para agir do ponto de vista da legalidade ou da ilegalidade, sem que o DPO o decida.

Nessa toada, como outrora concluído, deve-se ter por norte que a LGPD previu a "demonstração" pelo agente de tratamento quanto à adoção dessas medidas para cumprimento das normas de proteção de dados e da eficácia dessas medidas. E isso significa que o princípio da prestação de contas determina que os agentes de tratamento provem a adoção e a respectiva eficácia dessas medidas, de modo que devem demonstrar por meio de relatórios, pautas, declarações, registros em plataformas e softwares, as medidas praticadas para observar a LGPD e a respectiva eficácia dessas medidas. O ideal aqui, portanto, é que o agente de tratamento documente todas essas medidas, de maneira a facilitar, portanto, essa comprovação exigida expressamente no inciso X.

Desse modo, sendo designado o encarregado pelo tratamento de dados pessoais e operando de maneira efetiva as suas funções, a documentação dos seus atos, para fins de prova, é de obrigatoriedade sob o ponto de vista do princípio da prestação de contas.

Devem, assim, ser documentados os atos praticados pelo DPO, nesse sentido, no exercício de suas funções, na esteira do § 2º do Art. 41 da LGPD, como forma de se prestar contas, logo, sobre o desempenho de suas atividades de maneira autônoma, sem interferências do agente de tratamento que o designa, para fins de cumprir o objetivo de assegurar aos titulares de dados todos os seus direitos insculpidos no sistema de proteção enveredado pela LGPD e demais normas que os assegurem.

Aliás, como já ponderado acima, orienta o Conselho Europeu, quanto à documentação dos pareceres do EPD, o seguinte:

> Se o responsável pelo tratamento ou o subcontratante tomar decisões incompatíveis com o RGPD e o parecer do EPD, deve ser dada a possibilidade ao EPD de transmitir de forma clara o seu parecer divergente ao mais alto nível da direção e a quem tomou as decisões.

Aqui fica clara a importância da documentação dos atos do DPO, para que possa exercer de forma autônoma as suas funções: como deve agir para impor a legalidade no tratamento dos dados pessoais promovido pela organização, em prol de assegurar os direitos dos titulares de dados, assume relevância a essa autonomia a documentação de suas recomendações mormente para que na hipótese em que o agente de tratamento opte (decida) por descumprir a LGPD, fique materializada a orientação ofertada pelo DPO em sentido contrário.

Documentar os atos do DPO, assim, é um dever da organização, porque do contrário, estaria a infringir o princípio da prestação de contas, consubstanciado no Art. 6º, inciso X, da LGPD, e, não o fazer, ainda pode trazer dúvidas quanto à existência de efetiva autonomia conferida ao DPO que em favor da organização funcione.

Logo, no sistema jurídico brasileiro de proteção de dados pessoais, o DPO deve atuar com autonomia, sem a qual o exercício de suas funções poderá ficar comprometido e ser efetivado de maneira distante do que idealiza a LGPD, somando-se a isso a documentação dos seus atos, que é obrigatória, sob o ponto de vista do princípio da prestação de contas, e ainda constitui uma maneira de comprovar que a organização de fato garante autonomia à atuação do encarregado de proteção de dados pessoais.

4.7 Responsabilidade civil e penal

Nesta seção se pretende analisar, primeiro, do ponto de vista cível, como se dá a responsabilidade do DPO, é dizer, perante quem responde pelos atos que pratica, e, em seguida, os regimes de responsabilidade a que pode se submeter. Posteriormente, analisa-se a responsabilidade do DPO no âmbito penal.

Questão que parece ser unânime, diante das disposições da própria LGPD, e por corroboração da literatura especializada, é o fato de que o encarregado de proteção de dados não possui responsabilidade pelo tratamento de dados operado pela organização diante dos titulares de dados ou frente à Autoridade Nacional de Proteção de Dados. Conforme argumentam Cots e Oliveira (2018, p. 220-221):

> Assim, segundo a nova lei, o encarregado não responderá civilmente perante os titulares ou à autoridade nacional em relação a tratamento de dados realizados pelo controlador, pois, é este último que concentra todo o poder decisório sobre o tratamento de dados, atuando o encarregado, apenas, como comunicador de tais decisões aos terceiros interessados.

No mesmo sentido assevera Bruno (2019, p. 317):

> No tocante à responsabilidade do Encarregado pelo Tratamento de Dados Pessoais em face de uma eventual não conformidade da empresa com os requisitos de proteção de dados, como regra geral, esta inexiste. O Encarregado não é pessoalmente responsável, pois o controlador e o operador são responsáveis por garantir e demonstrar que suas atividades são conduzidas de acordo com a regulamentação, de modo que a conformidade com a legislação aplicável à proteção de dados pessoais é uma responsabilidade do controlador e do operador, e não do Encarregado.

Na esteira das ponderações de tais autores, somando-se a tudo quanto aqui já se visualizou sobre o papel a ser desempenhado pelo *data protection officer*, fica claro que este não decide sobre as finalidades e meios de tratamento de dados pessoais, o que, aliás, nem pode ser conteúdo de outra função caso a exerça em favor da organização na qual funciona como DPO, assim, a sua atividade é se comunicar, intermediar, as relações entre o agente de tratamento e titulares de dados e ANPD, e orientar toda a organização para que o tratamento de dados pessoais seja operado em conformidade com a LGPD, mas não lhe incumbe decidir pela organização, senão orientar-lhe a fazê-lo sob os ditames da legalidade – e, optando-se por agir dentro da legalidade ou da ilegalidade, tal decisão deve ser reservada tão somente ao controlador/operador.

E, nesse sentido, caso o EPD pratique qualquer ato que possa constituir ilícito, o controlador ou operador que sejam seus contratantes, responderão na forma do CC, Art. 932, III, dispositivo segundo o qual é responsável pela reparação civil “o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele”.

Entretanto, cabe analisar os regimes de responsabilidade a que poderá se submeter o DPO frente ao agente de tratamento, o que irá variar conforme o tipo de relação contratual que venha a manter frente ao seu contratante.

Conforme argumentam Cots e Oliveira (2018, p. 221-222), o DPO, sendo empregado do agente de tratamento, responderá na forma da CLT (Consolidação das Leis do Trabalho), Art. 462, respondendo, portanto, perante o seu empregador, somente na hipótese de dolo, conforme enuncia o § 1º de referido dispositivo (BRASIL, 1943).

Por sua vez, o encarregado de proteção de dados que não seja empregado, como sugerem Cots e Oliveira (2018, p. 222), será responsabilizado na forma dos

Arts. 186, 187 e 927 do CC. Quer dizer, responderá pelo ilícito que praticar, de forma dolosa ou culposa, e, ainda, na hipótese de abuso de direito.

Aqui, deve-se entender tanto as pessoas naturais quanto as pessoas jurídicas que prestem serviços à organização, hipóteses nas quais se vislumbrará uma relação civil, não uma relação de emprego, conforme apontado anteriormente.

E, nesse sentido, caso o agente de tratamento tenha sido responsabilizado por ato praticado pelo DPO, assegurado lhe estará o exercício de direito de regresso, na forma do CC, Art. 934, o qual enuncia que “Aquele que ressarcir o dano causado por outrem pode reaver o que houver pago daquele por quem pagou, salvo se o causador do dano for descendente seu, absoluta ou relativamente capaz”. Dessa forma, ao agente de tratamento caberá regressar em face do DPO pelo ato ilícito ou pelo abuso de direito praticado.

Ressalta-se que à ANPD foi atribuída a prerrogativa de complementar o regime a que se submete o DPO, de maneira a pormenorizar a sua definição e atribuições, como autoriza o Art. 41, § 3º, da LGPD, o que, quando concretizado, poderá auxiliar a compreensão a respeito da responsabilidade no exercício de suas funções.

Via de consequência, o DPO não responde pela inobservância das normas afeitas à proteção de dados pessoais em que possa eventualmente incorrer o agente de tratamento, até porque, como visto, é este o responsável pela tomada de decisão quanto à matéria, a caber ao encarregado orientar a adoção de práticas com vistas ao cumprimento do sistema jurídico de proteção de dados pessoais. E, ainda que pratique atos ilícitos em sua atividade, o DPO por eles não responde diretamente, cuja responsabilidade será do agente de tratamento. De outra mão, o encarregado de proteção de dados pessoais poderá responder diante de seu contratante, o agente de tratamento de dados, conforme seja sua relação de emprego ou uma relação civil, cabendo ao agente de tratamento eventual exercício de direito de regresso em face do DPO.

No que tange à responsabilidade do DPO no âmbito penal, Cots e Oliveira (2018, p. 223), ponderam que: “Na esfera criminal, havendo cometimento de crime, responderá a pessoa que tenha praticado o ato típico, nos termos do artigo 13 do CP (Código Penal)”.

Trata-se, aqui, de pôr a análise a relação de causalidade entre a prática (comissiva ou omissiva em suas diversas modalidades) do DPO no exercício de suas funções. Conforme dispõe expressamente o Art. 13 do CP: “O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido” (BRASIL, 1940).

Ademais, a LGPD não prevê a circunstância da prática de crimes pelo DPO quando do desempenho de suas funções, de forma que a legislação penal deve ser aplicada em sua suficiência para proteger os bens jurídicos envolvidos em sua atividade.

Dessa maneira, pode-se depreender que nada obsta que o DPO responda por eventual prática de crime, desde que, evidentemente, haja o nexo entre o resultado e a sua ação ou omissão, como regularmente se aplica a legislação penal. É por isso que Cots e Oliveira (2018), quanto ao tema, ensinam que:

> Do ponto de vista do encarregado, para que este tome precauções quanto à sua responsabilização, excluindo-se, obviamente, os casos de má-fé e dolo, ele deverá se cercar de meios que validem sua atuação, ou, ainda, que preservem as instruções recebidas pelo controlador. Solicitar instruções por escrito, em formato que permita a preservação, pode ser de vital importância para a manutenção de seus direitos.

As ponderações dos autores trazem novamente à tona a aplicação do princípio da prestação de contas, que pode ser traduzido na documentação dos atos relacionados ao tratamento de dados pessoais, conforme dispõe o Art. 6º, inciso X, da LGPD.

Por exemplo, pode-se pensar na circunstância em que o DPO é consultado sobre determinada prática que, além de violar a LGPD também gere o potencial de ser praticado certo crime em espécie e, neste caso, o DPO recomende que o tratamento de dados não seja promovido do modo consultado pela organização. Na circunstância em que, posteriormente, se possa apurar a prática de crime, o DPO estará isento de responsabilidade no âmbito criminal e, tendo havido a documentação dos atos, ainda deterá meios probatórios para infirmar eventual acusação em referido sentido.

Via de consequência, não há previsão específica na LGPD relacionada à responsabilidade criminal do DPO, de maneira a preponderar a aplicação regular da legislação penal, sem especificidades, ressaltando-se que a documentação dos atos, respaldada pelo princípio da prestação de contas, na forma do Art. 6º, inciso X, da LGPD constitui essencial procedimento a ser adotado para que o DPO possa assegurar os seus direitos e materializar a realidade, inclusive, para eventual necessidade de defesa em procedimentos penais.

5 CONCLUSÃO

O direito à proteção de dados pessoais se insere no contexto da economia da informação, na qual a informação passa ser o bem de valor central, na qual cada vez mais os bens materiais se reduzem e são convertidos para bits, a potencializar, dessa forma, o acúmulo de informação e a velocidade de sua transmissão.

Nesse contexto, entretanto, situações põem à prova o Direito, diante dos riscos que passam a emergir nessa economia totalmente informada e integrada, na qual o risco passa a ser distribuído frente a todos, a exemplo dos filtro-bolha, que limitam o conteúdo dos usuários, de forma a vedar-lhes conteúdos variados e os inserirem em um contexto no qual os conteúdos buscados repetem-se e se afunilam para que não deixem de ser consumidos.

No Brasil, as tecnologias da informação se encontram em expansão, tanto para empresas, quando na análise da presença em domicílios, sobretudo em relação ao acesso à internet por meio de *smartphones*, encontrando-se o comércio eletrônico também em crescimento constante.

O direito à proteção de dados pessoais tem por seu precursor, entretanto, o direito à privacidade, enunciado no primeiro debate jurídico-doutrinário ainda no século XIX, por Warren e Brandeis, que abordaram o tema no ano de 1890, em publicação nominada *The right to privacy*, estudo que marcou a institucionalização do direito à privacidade.

Após isso, diversos documentos internacionais passaram a abordar o direito à privacidade: a Declaração Americana dos Direitos do Homem (1948); a Declaração Universal dos Direitos Humanos (1948); a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (1950); o Pacto Internacionais sobre Direitos Civis e Políticos (1966); a Conferência nórdica sobre direito à privacidade (1967). Assim, consolidou-se o direito à privacidade no cenário internacional, como um direito humano fundamental de primeira dimensão, e no Brasil, foi abordado na Constituição Federal em seu Art. 5º, inciso X.

Por sua vez, o direito à proteção dos dados pessoais pode ser visto como originário do direito à privacidade, mas cujo conteúdo com este não poderia mais ser confundido, tendo em vista que o direito à privacidade pressupõe em seu conceito uma distinção entre público e privado, com vistas a resguardar ao indivíduo certos aspectos contra a sua publicização, ao passo que o direito à proteção de dados, em seu conceito, consubstancia direitos que não abarcam tal discussão, de modo a haver

direitos cuja proteção dos dados pessoais se pretende de caráter eminentemente público.

E não data de hoje a proteção dos dados pessoais. Institucionalizada pioneiramente em 1970 na Alemanha, passou o direito à proteção de dados pessoais a se amplificar a diversos países, no que se pode chamar de gerações de leis sobre proteção de dados pessoais: a primeira, no início da década de 1970, com o objetivo de controlar a criação de bancos de dados para usos estatais; na segunda metade da década de 1970, focada no fenômeno computacional; a terceira, na década de 1980, para garantir efetividade ao cidadão quanto ao exercício da liberdade em relação ao tratamento de seus dados pessoais, mas ainda centrada no indivíduo; a quarta geração, correspondente às atuais Leis sobre a matéria, é caracterizada por focar o direito à proteção dos dados pessoais de modo a transpor o indivíduo, concebendo-o do ponto de vista coletivo.

A União Europeia, que já contava com a Diretiva 46, do ano de 1995, sobre proteção de dados pessoais, em 2016 aprovou a hoje tão conhecida *General Data Protection Regulation*, que teve influência direta na concepção da Lei Geral de Proteção de Dados brasileira.

No sistema jurídico brasileiro, entretanto, desde a Constituição Federal manteve disposições esparsas tocantes à proteção de dados pessoais, caso *habeas data*. E posteriormente o Código de Defesa do Consumidor, a Lei de Acesso à Informação e o Marco Civil da Internet também trouxeram importantes disposições sobre a matéria.

A concepção da LGPD, publicada em 2018, como mencionado, se deu diretamente por influência da aprovação da GDPR, tendo em vista que a GDPR impôs a observância às suas disposições a agentes de tratamento estrangeiros na hipótese de oferecimento de bens ou serviços ou realização de atividades de *profiling* relacionadas a cidadãos localizados na União Europeia, além de prever que qualquer transferência internacional de dados pessoais originários da União Europeia somente se admitiria para os países que adotassem garantias de proteção de dados pessoais equivalentes às da GDPR.

Nesse sentido, a LGPD foi concebida para assegurar os direitos de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, de modo a reger o tratamento de dados pessoais tanto em ambientes digitais quanto em meios

físicos, para o que buscou apresentar específicos fundamentos, princípios e elencar, ainda que exemplificativamente, os direitos dos titulares de dados.

Com vistas à proteção dos dados pessoais, a LGPD estabeleceu hipóteses taxativas nas quais poderá ser operado o tratamento de dados pessoais, as quais, inclusive, diversificam-se conforme se tratarem de dados pessoais simples ou dados pessoais sensíveis, e, também, estabeleceu diretrizes para a doção de medidas de segurança e boas práticas, além de conceber a criação da Autoridade Nacional de Proteção de Dados, em cujas funções está a fiscalização e promoção da aplicação da LGPD, inclusive, de modo a receber as reclamações diretamente dos titulares de dados pessoais.

Nesse contexto, se insere a figura do encarregado de proteção de dados, ou *data protection officer*, figura a ser indicada pelo agente de tratamento para zelar pela observância das operações de tratamento de dados pessoais sob os ditames do sistema jurídico de proteção de dados pessoais concebido pela LGPD. A figura do DPO já havia sido concebida há décadas, em 1977 na Alemanha, e passou a integrar a Diretiva 46 do Conselho Europeu, foi instituído de forma obrigatória na GDPR e, assim, foi institucionalizado na LGPD.

Na LGPD, as funções do DPO foram estabelecidas no Art. 41, § 2º, em seus respectivos incisos I, II e III. Como primeira função, lhe cabe o aceite de reclamações e comunicações ofertados pelos titulares de dados, a dever-lhes prestar esclarecimentos e adotar providências. Como segunda função, receber comunicações da ANPD e adotar providências. Em ambas, age como um intermediador entre os titulares de dados e a ANPD e o agente de tratamento que o designa. E como terceira função, deve orientar os funcionários e contratados sobre as práticas a serem adotadas quanto ao tratamento de dados pessoais.

Pode-se observar que as funções até então previstas para o DPO na LGPD não são mais restritas que as funções dispostas na GDPR, porquanto ao se realizar a leitura das funções estabelecidas no § 2º do Art. 41 em conformidade com os demais dispositivos da LGPD, como os seus princípios, fundamentos, boas práticas, direitos dos titulares, estas estão em equivalência com as funções atribuídas ao encarregado de proteção de dados na GDPR, e, assim, não deixam a desejar frente à norma europeia.

A LGPD, em sua redação atual, permite que tanto pessoas naturais quanto pessoas jurídicas possam desempenhar o papel de encarregado de proteção de

dados, o que segue, nesse sentido, a orientação dada para a aplicação da GDPR, modo a ser possível, assim, tanto indicar uma pessoa como DPO dentro da própria organização quanto fora dela, sendo essa pessoa externa uma pessoa natural ou uma pessoa jurídica.

Quanto à sua qualificação, também em consonância com a GDPR, o DPO deve conhecer o direito relacionado à proteção de dados pessoais, mormente a LGPD, dominar as suas implicações práticas, e ter conhecimento tanto teórico quanto prático relacionado à proteção de dados, sobretudo das atividades da organização em que irá funcionar, com capacidade plena para o exercício de suas funções, com aptidão para orientar as suas funções sob os princípios da proteção de dados, fazer cumprir os direitos dos titulares e poder exercer comunicação eficiente com a ANPD.

Entretanto, na designação do DPO pode surgir conflito de interesses na hipótese em que exerça outras atividades, sob outras funções, em favor da organização. Sob os paradigmas da GDPR, também, o que se pode concluir é que não há qualquer vedação para que o DPO cumule funções em favor da organização, independentemente de qual seja a sua relação com essa organização, seja como empregado ou um prestador de serviços externo, desde que se observe a impossibilidade de haver conflito de interesses entre a outra (ou outras) função exercida com a função de DPO, o que se pode consubstanciar na impossibilidade de que o DPO seja, em outra função, responsável por um tratamento de dados pessoais, de maneira a definir a finalidade e o modo do tratamento de dados em favor dessa organização.

Assume posição especial, nesse contexto, o conflito de interesses entre o advogado da organização que funcione ou pretenda funcionar como DPO, do que se pode arrematar que o advogado é livre para atuar também como DPO, desde que não existam incompatibilidades ou impedimentos nos termos do EAOAB. Entretanto, ao se analisar a cumulação de prestação de serviços de advocacia e de DPO em favor de uma mesma organização, haverá inafastável conflito de interesses porque o interesse perseguido pelo DPO é o do titular de dados, enquanto o interesse perseguido pelo advogado é o do seu cliente, que lhe contrata para promover a sua defesa em procedimentos judiciais ou administrativos, e, assim, defendê-lo, em seus interesses, ou para lhe apresentar as melhores soluções jurídicas, que lhe tragam benefícios, dentro da licitude, inclusive, diante de situações jurídicas em que haja entendimentos variados, conclusão esta, aliás, que está em consonância com a

paradigmática decisão da Ordem dos Advogados de Portugal, conforme parecer 14/99/2018-G, que concluiu pela incompatibilidade absoluta do exercício da função de DPO e da advocacia para uma mesma entidade, no âmbito não só da defesa em processos de qualquer natureza, mas também da consultoria jurídica, em favor da organização em que a pessoa funciona ou funcionou como DPO.

Já em relação à obrigatoriedade de indicação do DPO, esta é impositiva para o controlador, por expressa determinação do Art. 41 da LGPD. E até que haja determinação em sentido diverso, a indicação do encarregado é obrigatória para todo e qualquer controlador, o que poderá ser reformatado pela ANPD, à qual foi atribuída a faculdade de promover a dispensa de indicação do DPO, conforme a natureza, porte e volume de tratamento de dados – situação em que a ANPD poderá, assim, utilizar critérios objetivos, semelhantes aos da GDPR, para autorizar a dispensa do DPO.

E nesse sentido, na hipótese de desobrigação da indicação do DPO, é permitida a sua indicação de forma voluntária, caso em que o regime jurídico aplicado ao DPO de designação obrigatória deve ser igualmente observado e, ainda, de qualquer modo, todas as normas relativas à proteção de dados pessoais, presentes na LGPD ou não, são de observância imperativa àquele agente de tratamento dispensado da indicação do DPO.

Ainda, o DPO pode ser uma consultoria externa, especializada no exercício das funções de encarregado do tratamento de dados pessoais, desde que seja facilmente acessível, regularmente, conforme determina o Art. 41, § 1º da LGPD, e desde que às funções não haja qualquer prejuízo devido à circunstância de compartilhamento entre os vários agentes de tratamento que podem contratar a consultoria especializada, seja de pessoa natural, seja de pessoa jurídica.

Em consonância com as funções atribuídas pela LGPD, e sob o paradigma da GDPR, o DPO deve atuar com autonomia, sem ingerências do agente de tratamento que lhe indica à função, tendo acesso e envolvimento em todas as atividades de tratamento da organização em que funciona, com vistas a promover a observância do sistema de proteção de dados pessoais instituído pela LGPD, com o objetivo máximo e final de assegurar aos titulares de dados todos os seus direitos.

Documentar os atos praticados pelo DPO no exercício de suas funções é atividade obrigatória da organização, sob o ponto de vista do princípio da prestação de contas, e ainda constitui uma maneira de comprovar que a organização de fato garante autonomia à atuação do encarregado de proteção de dados pessoais.

Quanto ao tema da responsabilidade civil, pode-se concluir que o DPO não responde pela inobservância das normas afeitas à proteção de dados pessoais em que possa eventualmente incorrer o agente de tratamento, até porque, como visto, é este o responsável pela tomada de decisão quanto à matéria, a caber ao encarregado orientar a adoção de práticas com vistas ao cumprimento do sistema jurídico de proteção de dados pessoais. E, ainda que pratique atos ilícitos em sua atividade, o DPO por eles não responde diretamente, cuja responsabilidade será do agente de tratamento. De outra mão, o encarregado de proteção de dados pessoais poderá responder diante de seu contratante, o agente de tratamento de dados, conforme seja sua relação de emprego ou uma relação civil, cabendo ao agente de tratamento eventual exercício de direito de regresso em face do DPO.

Por fim, no que se refere à responsabilidade penal, não há disposição específica na LGPD. Todavia, responderá o DPO pela prática de crime em espécie desde que a ela tenha dado causa por ação ou omissão. A documentação dos seus atos aqui, novamente toma relevância, a fim de resguardar-lhe seus direitos frente a potencial procedimento penal para infirmar eventual acusação.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Malheiros Editores, 2015.

ALVES, Paulo. WhatsApp supera o Facebook e é o aplicativo mais popular do mundo. **TechTudo**. 2019. Disponível em: https://www.techtudo.com.br/noticias/2019/01/whatsapp-supera-o-facebook-e-e-o-aplicativo-mais-popular-do-mundo.ghtml.

ARAÚJO, Maria Cristina. **Os bancos de dados à luz do CDC**. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/261275/os-bancos-de-dados-a-luz-do-cdc. 2017.

ARAÚJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de Direito Constitucional**. 9. ed. rev. e atual. São Paulo: Saraiva, 2005.

ASSEMBLEIA geral das nações unidas. **Declaração universal dos direitos humanos**.1948.

ASSEMBLEIA geral das nações unidas. **Pacto Internacional sobre Direitos Civis e Políticos**.1966.

BARIFOUSE, Rafael. Como o WhatsApp ganha dinheiro?. **BBC News Brasil em São Paulo**. 2018. Disponível em: https://www.bbc.com/portuguese/geral-44009510.

BASTOS, Carlos Ribeiro; MARTINS, Ives Gandra. **Comentário à Constituição do Brasil**. 2. ed. v. 7. São Paulo: Saraiva, 2000.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRAMAN, Sandra. The micro and macroeconomics of information. ***Annual Review of Information Science and Technology*** (ARIST), 40, 3-52. Estados Unidos: Wiley Subscription Services, Inc., A Wiley Company, 2005.

BRASIL. **Decreto-Lei 2.848, de 7 de dezembro de 1940.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

BRASIL. **Decreto-Lei nº 5.452, de 1º de maio de 1943**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm.

BRASIL. **Constituição da República Federativa do Brasil**, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. **Lei nº 8.906, de 4 de julho de 1994**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8906.htm.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BRUNO, Marcos Gomes da Silva. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. In V. N. MALDONADO; R. O. BLUM (Orgs.), **Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2019, pp. 305-328.

BUCKLAND, Michael Keeble. ***Information as thing***. *Journal of the American Society for Information Science*, *New York*, v. 42, n. 5, p. 351-360, jun. 1991.

CASTELLS, Manuel. **A era da informação**: economia, sociedade e cultura. In: A Sociedade em rede. São Paulo: Paz e Terra, 2000. v. 1.

COMITÊ gestor da internet no brasil. Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras: **TIC empresas 2017**. Coordenação executiva Alexandre F. Barbosa. São Paulo: Comitê Gestor da Internet no Brasil, 2018.

COMITÊ gestor da internet no brasil. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: **TIC domicílios 2018**. Núcleo de Informação e Coordenação do Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2019.

CONFERÊNCIA nórdica sobre direito à privacidade. 1967.

CONSELHO da Europa da Corte europeia de direitos humanos. **Convenção europeia dos direitos do homem**. 1950.

CONSELHO europeu. **Orientações sobre os encarregados da proteção de dados (EPD)**. Adotadas em 13 de dezembro de 2016. Com a última redação revista e adotada em 5 de abril de 2017.
CONSELHO Federal da Ordem dos Advogados do Brasil. **Código de Ética e Disciplina da OAB**. 1995.

CONSELHO Geral da Ordem dos Advogados de Portugal. **Parecer 14/PP/2018-G de 28 de setembro, 2018**. Disponível em: https://portal.oa.pt/advogados/pareceres-da-ordem/conselho-geral/2018/processo-de-parecer-14pp2018-g/

COOLEY, Thomas McIntyre. ***A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract***. Chicago: Callaghan and Company, 1879.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais**: comentada. São Paulo: Thomson Reuters Brasil, 2018.

CRETELLA JÚNIOR, José. **Comentário à Constituição de 1988**: artigos 170 a 232. 2. ed. v. 8. Rio de Janeiro: Forense Universitária, 1993.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**. vol. 13. ano 4. p. 59-67. São Paulo: Ed. RT, out.-dez. 2017.

DANTAS, Marcos. Informação-valor e corporações-redes: elementos para discutir um novo padrão de acumulação. **Informare: Cadernos do Programa de Pós-Graduação em Ciência da Informação**, v. 3, n. 1/2, 1997. Disponível em: http://hdl.handle.net/20.500.11959/brapci/41665.

DECLARAÇÃO Americana dos Direitos do Homem, 1948.

DONEDA, Danilo. Princípios da Proteção de Dados Pessoais. In N. LUCCA; A. S. FILHO; C. R. P Lima (Coords.), **Direito & *Internet III:*** Marco Civil da Internet Lei 12.965/2014. São Paulo: Quartier Latin, 2015.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DOVE, Edward. S. ***The EU General Data Protection Regulation****: Implications for International Scientific Research in the Digital Era*. In *The Journal of Law Medicine & Ethics.* Dez. 2018, pp. 1013-1030.

FERNANDES, Pedro Onofre. Economia da informação. **Ciência da Informação**, v. 20, n. 2, p.165-168, 1991.

FÓRUM de Governança da Internet das Nações Unidas. **Carta de Direitos Humanos e Princípios para a Internet**. 2011. Disponível em: https://internetrightsandprinciples.org/charter/

FURLANETO NETO, Mário; GARCIA, Bruna Pinotti. **Da guarda de registro de acesso e aplicações de internet na provisão de aplicações**. In G. S. LEITE; R. LEMOS (Coord.) Marco Civil da Internet. São Paulo: Atlas, 2014.

GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora UNESP, 1991.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**. 9. ed. v. 3. São Paulo: Saraiva, 2012.

GOUVEIA, Luís Manuel Borges. **Sociedade da Informação: n**otas de contribuição para uma definição operacional. Disponível em http://www.ufp.pt/. 2004.

GUTIERREZ, Andriei. Capítulo IX – Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In V. N. MALDONADO; R. O. BLUM (Orgs.), **Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2019, pp. 387-402.

JIMENE, Camilla do Valle. Capítulo VII – Da Segurança e das Boas Práticas. In V. N. MALDONADO; R. O. BLUM (Orgs.), **Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2019, pp. 329-360.

LASTRES, Helena Maria Martins; FERRAZ, João Carlos. Economia da informação, do conhecimento e do aprendizado. In H. M. M. Lastres & S. Albagli (Orgs.), **Informação e globalização na era do conhecimento**. Rio de Janeiro: Campos, 1999, pp. 27-57.

LOPES, Mariana Louback L. Capítulo VII – Segurança e boas práticas. In B. FEIGELSON; Na. H. A. SIQUEIRA (Orgs.), **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Revista dos Tribunais, 2019, pp. 173-184.

MAGRANI, Eduardo. **Democracia conectada**: a internet como ferramenta de engajamento político-democrático. Curitiba: Juruá, 2014.

MALDONADO, José. Tecno-globalismo e Acesso ao Conhecimento. In H. M. M. Lastres & S. Albagli (Orgs.), **Informação e globalização na era do conhecimento**. Rio de Janeiro: Campos, 1999, pp. 105-121.

MALDONADO, Viviane Nóbrega. A Lei Geral de Proteção de Dados: objeto, âmbito de aplicação, requisitos, segurança e a necessidade de sua correta implementação. **Lei Geral de Proteção de Dados Pessoais**: manual de implementação. São Paulo: Revista dos Tribunais, 2019, pp. 11-34.

MELLO, Luã Maia de. Capítulo VI – Agentes de tratamento de dados pessoais. In B. FEIGELSON; Na. H. A. SIQUEIRA (Orgs.), **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Revista dos Tribunais, 2019, pp. 159-172.

MELO, Alcemara Carmem Borges. **A boa-fé objetiva e os efeitos da *supressio* e *surrectio* nos contratos cíveis**. Disponível em: http://www.egov.ufsc.br/portal/conteudo/boa-fé-objetiva-e-os-efeitos-da-supressio-e-surrectio-nos-contratos-cíveis.

MIRANDA, Leandro Alvarenga. **A proteção de dados pessoais e o paradigma da privacidade**. São Paulo: All Print Editora, 2018.

MORAES, Alexandre de. **Direitos humanos fundamentais**: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 7. ed. São Paulo: Atlas, 2006.

NEGROPONTE, Nicholas. ***Being digital***. Grã-bretanha, Mackays of Chatham PLC, Chatham, Kent, 1995.

OABPR. **Estatuto da advocacia e da OAB comentado**. PIOVEZAN, G. C.; FREITAS, G. T. O. Curitiba: OABPR, 2015.

PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados brasileira: uma visão otimista. **Revista do Advogado**. Ano XXIX. n. 144. nov. 2019. São Paulo: AASP.

PESSOA, Valton Doria. **A incidência do *venire contra factum proprium* nas relações de trabalho**. 2013. 196 f. Tese (Doutorado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2013.

PORCARO, Rosa Maria.; JORGE, Marina Figueiras. Economia da informação no Brasil. **Cadernos temáticos do observatório: economia da informação e internet**. Campinas: SOFTEX, 2013, pp. 39-67.

REALE, Miguel. **Teoria tridimensional do direito**. 5. ed. São Paulo: Saraiva, 1994.

RENNAN, Julio A. “Dados são o novo petróleo”, diz CEO da Mastercard – exceto por um pequeno detalhe. **Época negócios**. 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: privacidade hoje. Rio de Janeiro: Renovar, 2008.

SALDANHA, Nuno. **Novo regulamento geral de proteção de dados**: o que é? A quem se aplica? Como implementar? Lisboa: FCA, 2018.

SHAPIRO, Carl; VARIAN, Hal. R. ***Information rules: a strategic guide to the network economy***. Estados Unidos: Harvard Business School Press, 1999.

SILVA, José Afonso da. **Comentário contextual à Constituição**. São Paulo: Malheiros Editores, 2007.

SIQUEIRA, Antonio Henrique Albani. Capítulo I – Disposições preliminares. In B. FEIGELSON; Na. H. A. SIQUEIRA (Orgs.), **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Revista dos Tribunais, 2019, pp. 15-58.

TARTUCE, Flávio. **Direito Civil**. v. 3. 9. ed. rev. atual. ampl. São Paulo: Método, 2014.

TEMER, Michel. **Elementos de Direito Constitucional**. 3. ed. rev. at. São Paulo: Malheiros Editores, 1993.

TEJEDOR, Iciar López-Vidriero. et al. ***RGPD y su afectación práctica****: Nuevo Escenario – Nuevas Políticas.* Madrid: Fundación Confemetal, 2018.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046.

UNIÃO EUROPEIA. **Regulamento (CE) n.o 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679.

VAINZOF, Rony. Capítulo I – Disposições Preliminares. In V. N. MALDONADO; R. O. BLUM (Orgs.), **Lei Geral de Proteção de Dados Comentada**. São Paulo: Revista dos Tribunais, 2019, pp. 19-178.

VASCONCELOS, Beto; DE PAULA, Felipe. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In. TEPEDINO, G. et al (Coord.), **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, pp. 717-740.

VIEIRA, Tatiana Malta. ***O direito à privacidade na sociedade da informação:*** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 296 f. Dissertação (Mestrado em Direito, Estado e Sociedade). Universidade de Brasília, Brasília, 2007.

VOSS, W. Gregory. *European Union Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*. ***The Business Lawyer****.* v. 72. 2016-2017.

WARREN, Samuel Dennis.; BRANDEIS, Louis Dembitz. ***Harvard Law Review****.* V. 4. Ed. 5., pp. 193-220, 1890.

WIMMER, Mirian. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. In BIONI, B. R (Coord.), **Revista do advogado: Lei Geral de Proteção de Dados Pessoais**. N. 144, nov. 2019, pp. 126-133.

WOLFF, Rosane Portella. **A proteção da vida privada e o direito a informação**. Orientador: Osvaldo Ferreira de Melo. 1991. 169 f. Dissertação (Mestrado em Ciências Humanas - Especialidade Direito) - Universidade Federal de Santa Catarina, Florianópolis, 1991.