

A PROTEÇÃO DE DADOS PESSOAIS ENQUANTO DIREITO FUNDAMENTAL: CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

PERSONAL DATA PROTECTION AS A FUNDAMENTAL
RIGHT: CONSIDERATIONS ABOUT THE PERSONAL
DATA PROTECTION GENERAL LAW

LA PROTECCION DE DATOS PERSONALES EN CUANTO
DERECHO FUNDAMENTAL: CONSIDERACIONES
SOBRE LA LEY GENERAL DE PROTECCIÓN A DATOS
PERSONALES

SUMÁRIO:

Introdução; 1. Big Data; 2. Dado e informação; 3. A Lei geral de proteção de dados: o direito à proteção de dados como direito fundamental; 4. Considerações finais; Referências.

RESUMO:

A era da sociedade da informação e mais precisamente do *Big Data* traz ao centro da discussão a produção e manipulação de dados pessoais e os limites desse tratamento diante do envolvimento de direitos da personalidade. Motivado pela adoção de um regulamento geral de proteção de dados pessoais pela União Europeia, o legislador brasileiro aprovou a Lei Geral de Proteção de Dados, tornando expressamente a proteção de dados pessoais como um direito fundamental.

Como citar este artigo:
BOTELHO, Marcos.
A proteção de dados
pessoais enquanto
direito fundamental:
considerações sobre
a lei geral de proteção
de dados pessoais.
Argumenta Journal
Law, Jacarezinho – PR,
Brasil, n. 32, 2020,
p. 191-207.

Data da submissão:
22/01/2020

Data da aprovação:
01/04/2020

ABSTRACT:

The era of information society and, more precisely, the Big Data, brings into center of the debate them production and manipulation of personal data and the limits of this treatment regarding the involvement of personality rights. Motivated by the adoption of a general rule about personal data protection in European Union, de Brazilian legislator has approved the General Data Protection Law, making clearly the personal data protection as a fundamental right.

RESUMEN:

La era de la sociedad de la información y, más precisamente, de Big Data trae al centro de la discusión la producción y manipulación de datos personales y los límites de este tratamiento frente a la participación de los derechos de la personalidad. Motivado por la adopción de un reglamento general para la protección de datos personales por parte de la Unión Europea, el legislador brasileño aprobó la Ley General de Protección de Datos, expresamente haciendo de la protección de datos personales un derecho fundamental.

PALAVRAS-CHAVE:

LGPD; Dados pessoais; Direito Fundamental; Segurança da Informação.

KEY-WORDS

LGPD; personal data; Fundamental right; Information security.

PALABRAS CLAVE:

LGPD; Datos personales; Derecho fundamental; Seguridad de la Información.

INTRODUÇÃO

Vivemos na chamada “era da informação” em que dado e informação figuram como importante ativo das empresas para a consecução de suas atividades e objetivos.

Por outro lado, a produção de dados é igualmente um fenômeno pre-

sente nos dias atuais, havendo a necessidade de tratamento desses dados para a produção de informações que irão agregar valor às atividades econômicas em determinado segmento. Em outras palavras, “[...] os dados se tornaram matéria-prima dos negócios, um recurso econômico vital, usado para criar uma nova forma de valor econômico” (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 4).

A tecnologia não se afigura mais como um elemento secundário quando se fala em estratégia nos negócios. Portanto, o uso da tecnologia para a extração de volume, variedade e velocidade de dados é ponto fundamental para a estratégia de negócios.

Se, por um lado, há o interesse dos diversos setores da atividade econômica em utilizar dados para a consecução de seus objetivos estratégicos, existe, de outro lado, a preocupação com a proteção de dados pessoais, sobretudo porque envolve um direito fundamental.

Não se pode deixar de mencionar que a necessidade de proteção aos dados pessoais restou evidente por ocasião do vazamento de dados do Facebook-Cambridge Analytica, envolvendo cerca de 87 milhões de usuários.

A manipulação de dados pessoais pela empresa Cambridge Analytica teve forte impacto em dois eventos importantes, a saber, a eleição presidencial americana em 2016 e a votação do Brexit.

O caso Cambridge-Analytica teve influência na criação do Regulamento Geral de Proteção de Dados da União Europeia, que serviu de fundamento para a aprovação no Brasil da Lei nº 13.709, de 14 de agosto de 2018, a chamada Lei Geral de Proteção de Dados (LGPD).

O presente artigo objetiva discutir a proteção de dados pessoais enquanto direito fundamental à luz da disciplina instituída pela Lei Geral de Proteção de Dados. Para tanto, analisaremos primeiramente a ideia de *Big Data*, com vistas a contextualização do momento histórico em que a necessidade de proteção de dados pessoais surge. Em seguida, trataremos a definição de dados, informação e conhecimento, passando, após, a um estudo sobre a proteção de dados como direito fundamental da pessoa humana, terminando com a análise dos principais atores descritos na Lei Geral de Proteção de Dados (titular, controlador, operador, encarregado e a Autoridade Nacional de Proteção de Dados).

1. BIG DATA

Para entender a proteção de dados pessoais enquanto direito fundamental, faz-se necessário entender o contexto do *Big Data* e o seu impacto na sociedade.

Embora a importância dos dados e da informação não seja nova, é com a consolidação da sociedade digital que o seu papel irá assumir um protagonismo jamais visto na história da humanidade.

Etimologicamente o termo *Big Data* vai surgir no meio da década de 1990, utilizado pela primeira vez por John Mashey, um cientista aposentado, para se referir à manipulação e análise de um grande volume de dados (KITCHIN, 2014, p. 99).

Como afirmou Amaral (2016, p. 9), “[...] o elemento principal associado ao Big Data é o registro de qualquer fenômeno, natural ou não, em dados”. Essa capacidade de produção e registro de dados em larga escala é o que vai caracterizar o fenômeno do Big Data.

Assim, Big Data é “[...] a capacidade de uma sociedade de obter informações de maneiras novas a fim de gerar ideias úteis e bens e serviços de valor significativo” (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 2). Logo, o fenômeno do *Big Data* refere-se ao enorme crescimento na quantidade de dados produzidos no mundo¹.

Três dimensões básicas estão associadas ao *Big Data*. A primeira consiste no volume, já que há a necessidade de se realizar o tratamento e a análise de volumes de dados muito grandes. A segunda dimensão está associada à velocidade, pois o plexo de técnicas deverá possibilitar que as análises do grande volume de dados sejam feitas com agilidade. Por fim, a terceira dimensão consiste na variedade, pois há diversas fontes de dados, informações distintas formadas e que exigem tratamento adequado (GOLDSCHMIDT; PASSOS; BEZERRA, 2015, p. 211).

Neste contexto é que:

A quantidade de informação armazenada cresce quatro vezes mais rápido que a economia mundial, enquanto a capacidade de processamento dos computadores cresce nove vezes mais rápido. Todos são afetados pelas mudanças (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 6).

A informação passa a ser considerada como fator de produção em um contexto em que os dados são produzidos em uma velocidade vertigi-

nosa, exigindo-se uma gestão da informação, a saber, o método utilizado por uma organização qualquer para planejamento, coleta, organização, utilização, controle, disseminação e descarte de suas informações de maneira eficiente (HINTZBERGEN et. al., 2018, p. 56).

Na era da *Big Data*, o tratamento de dados é de fundamental importância para a prospecção de informações úteis, que agregarão valor à atividade econômica da organização. Segundo Mayer-Schönberger e Cukier (2013, p. 7), “[...] quando aumentamos a escala de dados com a qual trabalhamos, ganhamos margem para inovar, o que não era possível quando trabalhávamos com quantidades menores”.

Contudo, o aumento na quantidade de dados disponíveis para prospecção e problemas com a utilização desenfreada de dados pessoais não passou despercebido pelo sistema legal, que começou a responsabilizar inúmeras organizações em razão da ausência dos devidos cuidados com a segurança dos dados.

No Brasil, a Lei Geral de Proteção de Dados disciplinou o conceito de tratamento de dados, dispondo no artigo 5º, inciso X, *in verbis*:

Art. 5º *Omissis*.

[...]

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

No contexto do *Big Data*, o tratamento de dados pessoais passa a receber atenção especial da legislação, reconhecendo-se a posição vulnerável da pessoa. De acordo com a LGPD o tratamento abrange toda e qualquer operação que faça utilização de dados pessoais como matéria-prima (FEIGELSON; SIQUEIRA, 2019, p. 23)².

Com a possibilidade de análise de grande volume de dados não estruturados e em constante modificação, os dados pessoais passam a receber especial proteção jurídica, tendo em vista o potencial lesivo do seu uso indiscriminado.

Ademais, a Internet contribuiu de maneira decisiva para o processo de produção de dados. E, juntamente com a Internet, a disseminação de

dispositivos móveis funcionou como catalizador nesse processo de produção de dados. Assim:

O poder de armazenamento, os recursos computacionais e o acesso à internet oferecidos por esses dispositivos ampliaram não somente a quantidade de dados únicos gerados, mas também a quantidade de vezes que eles eram compartilhados (MARQUESONE, 2016, p. 5).

Esses dados produzidos são registrados, analisados e organizados, criando um fenômeno chamado de *dataficação* (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 54). Segundo Amaral (2016, p. 9):

Do ponto de vista tecnológico, o elemento principal associado ao Big Data é o registro de qualquer fenômeno, natural ou não, em dados. Esses dados são persistidos, armazenados para reprodução ou análise, sendo imediata ou futura. Tal fenômeno é conhecido como *datafication*. Em outras palavras, *datafication* é o registro eletrônico de um fenômeno qualquer.

O *Big Data* faz utilização de algoritmos e ferramentas aptas a processar grandes volumes de dados em tempo real. Volume, velocidade e variedade são as características desse fenômeno. Os dados não são estruturados, sendo voláteis, coletados em momento próximo em que são produzidos (SAMPAIO, 2018, p. 18).

Além dos atributos volume, velocidade e variedade, alguns estudiosos acrescentam outros dois, a saber, o valor que diz respeito a importância de um dado para a solução de um determinado problema, e a veracidade, relacionada à confiabilidade dos dados, pois grandes volumes de dados possuem muitos dados inconsistentes.

O fenômeno do *Big Data* permite a captura de dados de populações inteiras ou sistemas em sua quase totalidade, em volumes muito superiores àqueles empregados nas tradicionais análises de dados em pequena escala. Isso possibilita uma resolução que objetiva ser a mais detalhada possível. Segundo Amaral (2016, p. 12), “Big Data é o fenômeno de massificação de elementos de produção e armazenamento de dados, bem como os processos e tecnologias, para extraí-los e analisa-los.”

Por outro lado, há flexibilidade, já que a extensão dos dados pode ser modificada, pois é possível adicionar novos campos de análise com certa facilidade, com alto grau de escalabilidade, ou seja, capacidade de rápida

expansão (KITCHIN, 2014, p. 99).

2. DADO E INFORMAÇÃO

O fenômeno do *Big Data* revela a importância dos dados e das informações para as organizações no mundo contemporâneo. A tomada de decisões na atualidade é feita com base na coleta e tratamento de dados e a sua transformação em informações que agreguem valor para a organização.

Entender os conceitos de dado e informação é fundamental para o êxito no processo de tomada de decisões, sobretudo porque são noções distintas.

O advento da *Internet of Things (IoT)* e taxa de crescimento de dados no mundo que alcançará a impressionante marca de 44 zettabytes de informações digitais revela o quão importante é o armazenamento de grandes e múltiplas bases de dados.

A descoberta de conhecimento em bases de dados, com a utilização de ferramentas, como a mineração de dados e a elaboração de modelos preditivos, é diferencial essencial no mercado altamente competitivo.

Neste contexto, os dados representam o fato bruto, o elemento básico, sendo que o vocábulo “dado” é proveniente da palavra latina *datum*. Assim, “Os dados são fatos ou observações brutas, em geral sobre fenômenos físicos ou transações de negócios.” (O’BRIEN; MARAKAS, 2013, p. 32).

Dados, portanto, são os fatos que são coletados e armazenados, podendo se apresentar em formato eletrônico analógico ou digital (AMARAL, 2013, p. 3). O dado analógico consiste naquele que é transmitido por intermédio de ondas, podendo sofrer interferência eletromagnética; já o dado digital é transmitido através de pacotes de bits (AMARAL, 2013, p. 4).

Os dados representam objetos reais (STAIR; REYNOLDS, 2006, p. 4), podendo, ainda, serem estruturados e não-estruturados. Os primeiros são aqueles dados armazenados em formatos de fácil compreensão, como por exemplo, tabelas, diferentemente dos dados não-estruturados, que não possuem uma estrutura previamente definida, como é o caso de arquivos de música.

Eleutério (2015, p. 31) assevera que os dados são registros de algo

que foi observado e medido e que podem ser representados textualmente, visualmente ou de forma numérica. São fatos brutos e, embora possam se apresentar de forma estruturada, o dado por si só não possui valor significativo e útil.

Seu valor agregado é pequeno e depende de um processo de tratamento para extração de significado e utilidade. Logo, o dado é a matéria-prima da informação, sendo que esta última é o resultado do tratamento que é conferido a uma determinada base de dados.

Segundo Goldschmidt, Passos e Bezerra (2015, p. 3):

Os dados [...] podem ser interpretados como itens elementares, captados e armazenados por recursos da Tecnologia da Informação. São cadeias de símbolos e não possuem semântica (*i.e.*, significado). Seu propósito é expressar fatos do mundo real de forma a serem tratados no contexto computacional.

Os dados se tornam importante recurso organizacional na medida em que podem ser analisados e transformados em informação. A informação é o resultado do tratamento dos dados, a transformação do fato bruto, da representação de um fato da realidade, em valor para a organização.

A informação representa os dados que foram devidamente processados e analisados e que passam a ter um significado em certo contexto (HINTZBERGEN et. al., 2018, p. 53). O tratamento dos dados produz utilidade e agrega valor, permitindo que a tomada de decisões seja feita com base em elementos capazes de lhe conferir solidez.

Para Stair e Reynolds (2006, p. 4), a informação deve ser compreendida como um plexo de fatos brutos organizados e possuidores de valores adicional, sendo que “As regras e relações podem ser criadas para organizar dados com informações úteis e valiosas.” (STAIR; REYNOLDS, 2006, p. 5)

O valor econômico da informação está ligado ao tratamento dos dados e das relações que são estabelecidas nesse processo. Por esta razão, os dados podem assumir valores distintos conforme o contexto que se apliquem. Segundo Stair e Reynolds (2006, p. 5):

O tipo de informação criada depende das relações definidas entre os dados existentes [...]. O acréscimo de dados novos ou diferentes indica que relações podem ser redefinidas e no-

vas informações podem ser criadas.

O processo de transformação de dados em informação envolve ferramentas de análise, aplicação da matemática a grandes quantidades de dados (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 8), com tarefas que se relacionam de maneira lógica e que são feitas para a obtenção de um resultado definido (STAIR; REYNOLDS, 2006, p. 5).

Todavia, embora a informação contenha mais valor agregado, o dado também possui certo valor. Esta é a razão pela qual há necessidade de proteção de dados (HINTZBERGEN et. al., 2018, p. 55).

Por fim, o tratamento de dados, transformando-os em informação permite a obtenção de conhecimento, “[...] que corresponde a um padrão ou conjunto de padrões cuja formulação pode envolver e relacionar dados e informações” (GOLDSCHMIDT et. al., 2015, p. 3). Segundo Stair e Reynolds (2006, p. 5), “Conhecimento é a consciência e o entendimento de um conjunto de informações e formas de torna-las úteis para apoiar uma tarefa específica ou tomar uma decisão”.

3. A LEI GERAL DE PROTEÇÃO DE DADOS: O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

O cenário descrito nos tópicos anteriores deixa evidente a importância de dados e informações as organizações contemporâneas. Os dados, como ativos importantes, possibilitam a melhora da competitividade das organizações, na medida em que tornam possível a elaboração de modelos preditivos que auxiliarão em objetivos específicos e tarefas de tomada de decisões.

A outro prisma, a sociedade digital permite a formação de trilhas digitais que podem ser exploradas por organizações. Em outras palavras, interagir no meio digital produz rastros e dados, os quais podem ser objeto de análise e obtenção de informações.

É conhecido o fato de que uma análise de cinco compras no cartão de crédito pode revelar muito do perfil da pessoa. Mesma situação se dá com o comportamento de uma pessoa nas redes sociais.

Neste quadro, a pessoa natural encontra-se em evidente posição de vulnerabilidade, pois parte de seus dados pessoais estão à disposição de terceiros sem que ela tenha domínio sobre isso, colocando em risco a pri-

vacidade, intimidade e dados pessoais.

A Lei Geral de Proteção de Dados surge neste contexto para se colocar como o principal diploma legal sobre o tema no Brasil. Ela inclui fundamentos e princípios que vão para além do seu próprio texto, servindo como um norte para a interpretação e aplicação de leis que envolvam o tratamento de dados pessoais e sua proteção (COTS; OLIVEIRA, 2019, p. 39). Segundo Maldonado (2019, p. 12) “Não é preciso ser um especialista na área da privacidade para compreender a importância que a proteção de dados ostenta nos dias de hoje”.

Segundo o artigo 1º da Lei Geral de Proteção de Dados, a sua disciplina incide sobre o tratamento de dados pessoais, inclusive nos meios digitais (PINHEIRO, 2019, p. 50). Portanto, a LGPD não trata apenas dos dados em formato digital, abarcando as bases de dados físicas.

Um primeiro ponto a ser destacado, é que o destinatário da proteção legal é a pessoa natural. A expressão “dados pessoais” presente na redação do artigo 1º da LGPD traz esta limitação. A pessoa natural identificada ou identificável é o sujeito que receberá proteção da lei.

Esta ideia é reforçada pela disciplina contida no artigo 5º, inciso I da LGPD, *in verbis*:

Art. 5º Para os fins desta Lei, considera-se:

I – dado pessoal: informação relacionada a **pessoa natural** identificada ou identificável. (grifamos)

Para que determinada informação seja considerada um dado pessoal, estando abarcada pela LGPD, ela deve estar relacionada a uma pessoa natural, além de ser identificada ou identificável (FEIGELSON; SIQUEIRA, 2019, p. 18).

O critério adotado pela LGPD na definição de dados pessoais é o expansionista, isto é:

[...] não define apenas como pessoais os dados que, imediatamente, identifiquem uma pessoa natural (viés do critério reducionista), como poderia ser informações como o nome, número do CPF, imagem, etc., mas abarcou também os dados que tornam a pessoa identificável de forma não imediata ou direta (COTS; OLIVEIRA, 2019, p. 71).

Aqui se faz importante salientar que os “dados pessoais” referidos pela Lei Geral de Proteção de Dados abarcam tanto os dados em si

considerados como as informações resultantes do tratamento de dados, consoante a distinção feita no tópico anterior. Embora no campo da tecnologia e segurança da informação dado e informação sejam conceitos distintos, a LGPD não teve essa preocupação. Note-se que essa conclusão pode ser extraída da simples leitura do inciso I do artigo 5º da LGPD, que relaciona “dado pessoal” com a “informação relacionada a pessoa natural”.

Por outro lado, o artigo 4º da LGPD assevera que o diploma normativo não se aplica ao tratamento de dados pessoais que é realizado por pessoa natural com finalidades exclusivamente particulares e não econômicas, ao tratamento que é realizado para fins exclusivamente jornalísticos, artísticos, acadêmicos, segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Por fim, lei não se aplica ao tratamento de dados pessoais que sejam provenientes de fora do território nacional e que não sejam objeto de comunicação ou uso compartilhado de dados com agentes de tratamento nacionais ou, ainda, objeto de transferência internacional de dados com outro país que não o de proveniência e desde que o país de proveniência possua um grau de proteção de dados pessoais adequado ao disciplinado na LGPD.

Ainda, deve ser destacado que o artigo 12 da LGPD exclui do âmbito de incidência do diploma normativo os dados anonimizados, que são aqueles dados relativos a determinado titular que não possa ser identificado, levando-se em consideração a utilização de ferramentas técnicas razoáveis e disponíveis por ocasião do tratamento³. Há que se destacar, ainda, que dados anonimizados não podem ser confundidos com dados pseudoanonimizados. Aqueles não permitem reversão, diferentemente do que ocorre com os pseudoanonimizados, cuja reversão é possível através de técnica que esteja em posse do controlador (COTS; OLIVEIRA, 2019, p. 120).

Lembra Pinheiro (2019, p. 57) que:

A delimitação da aplicabilidade da lei em relação aos tipos de dados que são considerados regulados pela LGPD demonstra que o tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado.

A proteção aos dados pessoais ofertada pela LGPD tem como objetivo a proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. Neste sentido, a redação do artigo 17 da LGPD, *in verbis*:

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Isso significa que a interpretação das normas que delimitam a aplicabilidade da LGPD deve levar em consideração a natureza do bem tutelado, de modo que a incidência ou não da lei deva promover, ao máximo, o direito fundamental à proteção de dados pessoais. Logo:

A LGPD reconhece que, para que o cidadão seja capaz de controlar o fluxo de seus dados pessoais, é necessário lhe atribuir certos direitos subjetivos em face daqueles responsáveis pelo controle de tais dados (FEIGELSON; SIQUEIRA, 2019, p. 120).

Neste sentido é que o artigo 2º da LGPD dispõe sobre os fundamentos que subjazem à disciplina de proteção de dados, a saber, o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Verifica-se que “A proteção aos direitos fundamentais é bastante evidente no art. 2º da LGPD” (PINHEIRO, 2019, p. 53)

Da leitura do artigo 2º da LGPD combinado com o artigo 17 do mesmo diploma resta claro que o desiderato da lei não é obstar o desenvolvimento econômico e tecnológico, mas sim, harmonizar a ordem econômica, disciplinada na Constituição Federal, com os direitos fundamentais e o respeito à dignidade da pessoa humana.

A LGPD fornece fundamento legal para o tratamento de dados pessoais, proporcionando maior segurança jurídica para controladores e operadores, além de fixar bases claras para a proteção e garantia do direito fundamental à proteção de dados. Logo, “[...] se não houver base legal a um determinado tratamento, este não poderá ocorrer ou subsistir, sequer

na forma de armazenamento” (MALDONADO, 2019, p. 16). E afirma Pinheiro (2019, p. 19) dizendo que “[...] a proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países.”

Por este motivo, o tratamento de dados pessoais somente poderá ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular. Esse é o princípio da finalidade, havendo a vedação de tratamento realizado posteriormente e que não esteja compatível com as finalidades explicitadas (FEIGELSON; SIQUEIRA, 2019, p. 31).

A proteção ao direito fundamental ao tratamento de dados pessoais objetiva a redução de riscos no que tange a coleta e utilização futura de dados pessoais. A proteção abarca todo o ciclo de vida do dado, o que vai desde à coleta até o seu descarte, englobando diversas fases que devem ser desenvolvidas em conformidade com a LGPD.

Sendo dados pessoais, eles pertencem a seu titular, razão por que o desiderato da LGPD, a exemplo do que pode ser encontrado no Regulamento Geral de Proteção de Dados da União Europeia, que serviu de base para a norma pátria, é possibilitar que as pessoas naturais tenham maior controle e autonomia sobre os seus dados pessoais (FEIGELSON; SIQUEIRA, 2019, p. 30).

Além da pessoa natural como destinatária da proteção da lei, a LGPD enumera outros atores importantes nas relações jurídicas envolvendo o tratamento de dados pessoais.

O primeiro ator já mencionado é o titular, a saber, a pessoa natural a quem se referem os dados pessoais que serão objeto de tratamento. Conforme já salientado alhures, o titular é apenas a pessoa natural, havendo exclusão pela lei da pessoa jurídica.

A LGPD faz alusão, ainda, aos agentes de tratamento, que são o controlador, que pode ser pessoa natural ou jurídica, de direito público ou privado, que possui o poder decisório no que tange ao tratamento de dados pessoais, e o operador, que consiste na pessoa natural ou jurídica, de direito público ou privado, que tem a função de realizar o tratamento de dados pessoais em nome do controlador. O seja:

O controlador nada mais é do que o responsável pela coleta dos dados pessoais e por tomar todas as decisões em relação à forma e à finalidade do tratamento dos dados, ainda que

não realize diretamente o tratamento em questão (FEIGELSON; SIQUEIRA, 2019, p 21).

Ponto importante a ser destacado é que as atribuições pertencentes ao controlador e ao operador poderão estar a cargo da mesma pessoa (COTS; OLIVEIRA, 2019, p. 165). A LGPD não exige que controlador e operador sejam pessoas distintas, podendo haver a cumulação de funções (FEIGELSON; SIQUEIRA, 2019, p. 22).

Mas, nos casos em que é pessoa distinta, o operador deve proceder ao tratamento dos dados pessoais observando as instruções que são fornecidas pelo controlador, a quem, por seu turno, cumpre verificar a observância das próprias instruções e normas sobre a matéria. Segundo Cots e Oliveira (2019, p. 168):

A LGPD não estabelece como serão transmitidas as instruções do controlador ao operador, mas é certo que em toda a relação na qual um controlador delega a um operador o tratamento de dados pessoais sob sua responsabilidade, deverá estabelecer instrumentos claros para tal tratamento.

E nesta relação entre controlador e operador, há a exigência legal (artigo 37) de que sejam mantidos registros de toda e qualquer operação de tratamento de dados pessoais, especialmente quando a base legal seja o legítimo interesse.

Há, também, a figura do encarregado, que é pessoa indicada pelo controlador e cuja função é atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados. Embora a redação original da LGPD previa que o encarregado deveria ser uma “pessoa natural”, a nova redação conferida pela Medida Provisória nº 869/2018, convertida na Lei nº 13.853/2019 retirou esta exigência, passando a permitir que o encarregado seja pessoa natural ou jurídica, a critério do controlador (FEIGELSON; SIQUEIRA, 2019, p. 22).

O encarregado deve ser indicado pelo controlador, tendo este o dever de divulgar a identidade e todas as informações necessárias de contato do encarregado publicamente, de preferência em site eletrônico (FEIGELSON; SIQUEIRA, 2019, p. 22).

As atividades básicas do encarregado, segundo o § 2º do artigo 41 da LGPD são o de aceitar as reclamações e comunicações dos titulares, além de prestar esclarecimentos e adotar providências, e receber comunicações

da autoridade nacional e adotar providências, orientar os funcionários da entidade no que tange as práticas a serem adotadas em relação à proteção de dados pessoais, além de executar as demais atribuições que forem estabelecidas pelo controlador ou em normas complementares.

Por fim, ator importante previsto na LGPD é a figura da Autoridade Nacional de Proteção de Dados, que consiste em órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Uma leitura da LGPD mostra que o inciso XIX do artigo 6º traz a menção à “Autoridade Nacional”, enquanto que no Capítulo IX do diploma normativo a autoridade recebeu outro nome, a saber, “Autoridade Nacional de Proteção de Dados”. Não obstante, “[...] os termos ‘autoridade nacional’ e ‘Autoridade Nacional de Proteção de Dados’ são sinônimos para fins de aplicação da LGPD” (COTS; OLIVEIRA, 2019, p. 73)

A razão disso está no fato de que este ator estava previsto nos artigos 55, 56 e 57, os quais foram vetados, sendo que, posteriormente, com a Medida Provisória 869/2018 houve alteração do inciso XIX, revogando a previsão de que a autoridade nacional deveria fazer parte da administração pública indireta, vinculando-a diretamente à Presidência da República. Assim, o artigo 55-A prescreve, *in verbis*:

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados – ANPD, órgão da administração pública federal, integrante da Presidência da República.

Trata-se, portanto, de órgão da administração pública direta, possuidora de autonomia técnica (art. 55-B), cuja composição encontra-se disciplinada no artigo 55-C da LGPD.

4. CONSIDERAÇÕES FINAIS

Por envolver direitos da personalidade, a proteção de dados pessoais foi considerada pela União Europeia como um direito fundamental, passando a merecer proteção jurídica adequada.

A Lei Geral de Proteção de Dados no Brasil, tendo por base o Regulamento Geral de Proteção de Dados da União Europeia, trilhou a mesma senda, deixando clara a intenção do legislador pátrio em considerar a proteção de dados pessoais como um direito fundamental do titular, a saber,

a pessoa natural.

Por outro lado, segurança e prevenção passam a ser duas premissas básicas na lógica da proteção de dados pessoais, haja vista que enquanto direito fundamental, a proteção de dados pessoais exige a implementação de medidas efetivas para a segurança no tratamento de dados.

A proteção de dados pessoais somente ocorrerá se houver a observância dos critérios legais previstos na LGPD no que tange a inserção de medidas necessárias à garantia da segurança do tratamento de dados pessoais, proteção que deverá abarcar todo o ciclo de vida dos dados.

Outrossim, importante destacar, como visto, que a expressão “dados” utilizado na lei não pode ser interpretada restritivamente. No âmbito da Tecnologia da Informação os termos “dado” e “informação” expressam conceitos distintos, sendo este o resultado do tratamento daquele.

Para os fins da Lei Geral de Proteção de Dados, os dados pessoais abarcam tanto o dado em sentido estrito quanto a informação obtida, na medida em que o desiderato principal da lei é a proteção de direito fundamental ligado à personalidade, a intimidade e privacidade.

Logo, tanto a manipulação de dados quando as informações produzidas a partir deles recebe a proteção da Lei Geral de Proteção de Dados, exigindo-se condutas de controladores, operadores e encarregados para o fomento de uma maior segurança da informação.

REFERÊNCIAS

AMARAL, Fernando. *Introdução à ciência de dados*. Rio de Janeiro: Alta Books, 2016.

BOTELHO, Marcos César. *A legitimidade da jurisdição constitucional no pensamento de Jürgen Habermas*. São Paulo: Saraiva, 2010.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de dados pessoais comentada*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

ELEUTÉRIO, Marco Antonio Masoller. *Sistemas de informações gerenciais na atualidade*. Curitiba: Intersaberes, 2015.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). *Comentários à lei geral de proteção de dados: Lei 13.709/2018*. São Paulo: Revista dos Tribunais, 2019.

GOLDSCHMIDT, Ronaldo; PASSOS, Emmanuel; BEZERRA, Eduardo. *Data mining: conceitos, técnicas, algoritmos, orientações e aplicações*. 2. ed. Rio de Janeiro: Elsevier, 2015.

HINTZBERGEN, Jule et. al. *Fundamentos de segurança da informação: com base na ISSO 27001 e na ISSO 27002*. Rio de Janeiro: Brasport, 2018.

KITCHIN, Rob. *The data Revolution: big data, open data, data infrastructure & their consequences*. Thousand Oaks: Sage Publications, 2014.

MALDONADO, Viviane Nóbrega (coord.). *LGPD: Lei Geral de Proteção de Dados Pessoais: manual de implementação*. São Paulo: Revista dos Tribunais, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords). *Comentários ao GDPR: Regulamento geral de proteção de dados da União Europeia*. São Paulo: Revista dos Tribunais, 2018.

MARQUESONE, Rosângela. *Big data: técnicas e tecnologias para extração de valor dos dados*. São Paulo: Casa do Código, 2016.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana*. Rio de Janeiro: Elsevier, 2013.

O'BRIEN, James A.; MARAKAS, George M. *Administração de sistemas de informação*. 15.ed. Porto Alegre: AMGH, 2013.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)*. São Paulo: Saraiva, 2019.

SAMPAIO, Cleuton. *Data Science para programadores: um guia completo utilizando a linguagem Python*. Rio de Janeiro: Ciência Moderna, 2018.

STAIR, Ralph M.; REYNOLDS, George W. *Princípios de sistemas de informação*. São Paulo: Pioneira Thomsom Learning, 2006.

'Notas de fim'

1 Basta dizer que a Google processa mais de 24 petabytes de dados diariamente (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 5).

2 Dados pessoais consistem em toda e qualquer informação que se relacione a uma pessoa natural identificada ou identificável.

3 Art. 5º, inciso III, da LGPD, in verbis: “Art. 5º Para fins desta Lei, considera-se: [...] III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.”

