REVISTA | DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NA LGPD

THE PROCESSING OF PERSONAL DATA BY THE PUBLIC AUTHORITY IN LGPD

Recebido em:	01/05/2021
Aprovado em:	27/10/2021

Marcos César Botelho[1]

Elimei Paleari do Amaral Camargo[2]

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. Recentes casos de abuso no tratamento de dados pelo Poder Público revelam a importância da disciplina de proteção de dados pessoais pelos órgãos da administração pública. Com a utilização de um método dedutivo e de pesquisas bibliográfica e exploratória como procedimentos técnicos, buscou-se analisar a disciplina, prevista na Lei Geral de Proteção de Dados Pessoais (LGPD), acerca do tratamento de dados pessoais pelo Poder Público.

Palavras-chave: LGPD; Dados pessoais; Segurança da Informação; Poder Público

[1] Doutor em Direito Constitucional no programa da Instituição Toledo de Ensino/Bauru-SP; Mestre em Direito Constitucional pelo Instituto Brasiliense de Direito Público; Professor adjunto vinculado ao programa de mestrado em ciências jurídicas na Universidade Estadual do Norte do Paraná (UENP). Endereço eletrônico: mc_botelho@yahoo.com.br

[2] Doutora em Educação pela UNIMEP; Mestre em Direito pela UNAERP; Professora Adjunta no curso de Direito na Universidade Federal de Rondônia - Câmpus de Cacoal. Endereço eletrônico: elimei@unir.br

ABSTRACT

The era of the information society and more precisely of Big Data brings to the center of the discussion the production and manipulation of personal data and the limits of this treatment in the face of the involvement of personality rights. Recent cases of abuse in the processing of data by the Public Power reveal the importance of the discipline of protection of personal data by public administration bodies. Using the deductive method and bibliographic and exploratory research as technical procedures, we sought to analyze the discipline provided for in the LGPD regarding the processing of personal data by the Government.

Key-words: LGPD; personal data; Information security; Public Administration

1 INTRODUÇÃO

A expansão dos dispositivos eletrônicos no cotidiano das pessoas e a conexão destes com a rede mundial de computadores levou a vigilância a figurar como uma dimensão central da modernidade (BAUMAN, 2013, p. 11).

O controle do fluxo de dados revela um mundo no qual o poder passa a existir em um espaço global e extraterritorial. Monitorar, coletar dados a fim de prever comportamentos, atuar sobre o enxame digital (HAN, 2018, p. 27) tem sido um fato frequente na sociedade da informação. A pandemia causada pelo COVID-19 trouxe a necessidade de tratamento de dados sensíveis pelo Poder Público para fins de implementação de políticas de saúde pública, expondo a vulnerabilidade dos cidadãos diante do aparato de vigilância estatal.

O Poder Público, como maior detentor de informações e dados pessoais, tem invadido a esfera da liberdade, da privacidade e do livre desenvolvimento da personalidade natural sempre com a justificativa com base em prioridades absolutas do presente que atuam como imunizantes das inúmeras violações levadas a cabo pelo Poder Público no tratamento de dados pessoais.

No Brasil, recentemente, o Supremo Tribunal Federal teve a oportunidade de apreciar normativo que autorizava o compartilhamento de dados pessoais de usuários de telefonia com o IBGE. Justificava-se o compartilhamento pela necessidade de produção estatística oficial durante a pandemia do COVID-19. O Pretório Excelso afastou a possibilidade deste compartilhamento evocando normas constitucionais e da própria LGPD como impeditivas da prática pretendida pelo Poder Público.

Outro caso no Brasil foi a tentativa da empresa Via Quatro, concessionária da Linha 4 – Amarela do metrô em São Paulo de coletar dados de som e imagem dos usuários através de câmeras instaladas nas estações. A Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14 de agosto de 2018 – entrou em vigor no dia 18 de setembro de 2020, representando um importante passo do Brasil no sentido de possuir uma norma que discipline o tratamento de dados pessoais, protegendo os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural.

A LGPD traz princípios que devem ser observados, bases legais que permitem o tratamento de dados pessoais, direitos do titular dos dados, além de prever no Capítulo IV, dividido em duas seções, sobre o tratamento de dados pessoais pelo Poder Público. O presente estudo se propõe a analisar as normas relativas ao tratamento de dados pessoais pelo Poder Público disciplinadas na Lei Geral de Proteção de Dados, buscando compreender quais as hipóteses permissivas de tratamento de dados pelas pessoas jurídicas de direito público.

Para tanto, foi utilizado o método dedutivo, tendo em vista que o ponto de partida para a análise da disciplina específica do Poder Público foram os princípios gerais incidentes sobre a Administração Pública estabelecidos na Constituição Federal e na LGPD, havendo, ainda, a utilização da pesquisa bibliográfica e a pesquisa exploratória como procedimentos técnicos adequados à execução do método escolhido.

REVISTA | DIREITOS SOCIAIS E POLÍTICAS PÚBLICAS (UNIFAFIBE)

2 A PROTEÇÃO DE DADOS NO CONTEXTO DO *BIG DATA, DA IOT E DA DATAFICAÇÃO*

Uma frase muito repetida nos dias atuais – "*Dados são o novo petróleo*" –, creditada a Clive Humby, matemático londrino especializado em Ciência de Dados reflete bem a importância que os dados passaram a ter para as organizações contemporâneas. Diferentemente do petróleo, que é uma fonte energética limitada e escassa, os dados não possuem essa característica e a evolução na quantidade de dados produzida no mundo aponta para esse cenário.

Logo, "[...] *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). Basta dizer que em 2007 cerca de 300 exabytes de dados estavam armazenados, sendo que aproximadamente 93% já se apresentavam em formato digital. Em 2020 estima-se que será alcançada a impressionante marca de 44 zettabytes de informações digitais. É neste cenário 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 (MAYER-SCHÖNBERGER; CUKIER, 2013, p. 6).

Há um cenário muito favorável à produção e armazenamento de dados, composto pela ocorrência simultânea dos fenômenos do *Big Data*, da Dataficação e da Internet das Coisas (IoT). São fenômenos que possuem forte ligação entre si e que montam um desenho social, econômico e político favoráveis à adoção de modelos que trabalhem com a produção e armazenamento de dados. O *Big Data* é compreendido como uma oportunidade de negócios. Sua definição parte de um conjunto de três "Vs", que expressam as ideias de volume, velocidade e variedade (AMARAL, 2016, p. 7). O termo *Big Data* aplica-se a grandes volumes

de dados armazenados, demandando a utilização de métodos distintos daqueles utilizados para o tratamento em base de dados tradicionais.

> O conceito de Big Data nada mais é do que a representação de um novo momento da sociedade, quando diversas mudanças de tecnologia acabaram por gerar uma profunda produção de dados, de variados tipos e com volumes e velocidades de dimensões diferentes. (BARBIERI: 2019, P. 107)

O fenômeno da Dataficação implica no registro digital de todo e qualquer fenômeno (AMARAL, 2016, p. 10). Em outras palavras, a "[...] *dataficação pode ser definida como a crescente centralidade dos dados na vida cotidiana, afetando os processos comunicacionais*" (GROHMANN, 2019, p. 106). A dataficação expressa o processo de transformação de todos os aspectos da vida em dados (SCHUTT; O'NEIL, 2014, p. 5), característica que na sociedade digital implica no fato de que o nosso comportamento no ambiente virtual sempre produzirá dados e gerará trilhas digitais.

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.

A Internet das Coisas (IoT) refere-se ao aumento da comunicação entre máquinas através da internet. Essa comunicação entre objetos ou M2M (machine-to-machine)

ultrapassou em volume a comunicação interpessoal na Internet (MAGRANI, 2018, p. 11) e integra o contexto da hiperconectividade:

> O termo hiperconectividade está hoje atrelado às comunicações entre indivíduos (person-to-person, P2P), indivíduos e máquina (human-to-machine, H2M) e entre máquinas (machine-to-machine, M2M) valendo-se, para tanto, de diferentes meios de comunicação (MAGRANI, 2018, p. 21).

Ademais, essa conexão de coisas com a internet traz uma impressionante capacidade para processamento, armazenamento, análise e compartilhamento de um volume de dados considerável, sendo que esses dispositivos serão produtores de dados (AMARAL, 2016, p. 13). O cenário, portanto, é de produção massiva e veloz de dados possibilitando o uso de ferramentas para a extração de informação que poderá ser utilizada para gerar dividendos econômicos para as organizações contemporâneas. Ou seja, "*A capacidade de processamento de dados se transformou em preceito nuclear para a evolução econômica*" (MALDONADO; BLUM, 2019, p. 38) e:

> A sociedade que consegue ter a abertura necessária para manipular dados, inovando e gerando novos modelos de negócios, produtos e serviços, automaticamente provoca o desenvolvimento e, consequentemente, alavanca a economia (MALDONADO; BLUM, 2019, p. 38).

No contexto de valorização dos dados pessoais, *Big Data*, Dataficação e IoT a exposição de dados pessoais ao uso indiscriminado é uma realidade a qual não se pode dar as costas,

principalmente porque a ausência de limites claros e objetivos à sua utilização representa ameaça à direitos fundamentais como a privacidade, intimidade e à direitos da personalidade. A existência de inúmeros dispositivos conectados e presentes na vida cotidiana da pessoa proporciona uma coleta, armazenamento e compartilhamento de dados que na maior parte das vezes não está sob o controle do titular dos dados pessoais. E esse processo de coleta e compartilhamento de dados ignora o fato de que muitos desses dados refletem questões particulares e íntimas do indivíduo com consequências para a privacidade, intimidade e segurança das pessoas (MAGRANI, 2018, p. 24).

Como afirmou BARBIERI (2019, p. 7), "*os dados, diferentemente de outros ativos organizacionais, podem ser copiados ou replicados*", característica que permite o seu tratamento veloz, devido à sua alta latência e as demandas da sociedade digital no que tange ao registro e processamento de dados bem próximos ao momento de sua ocorrência (BARBIERI, 2019, p. 13)[3]. Isso permite, por exemplo, a identificação no Brasil de cerca de 87% das pessoas dispondo apenas da data do nascimento, número do CPF e a idade, lembrando que cerca de 116 milhões de pessoas no Brasil estão conectadas na Internet e, portanto, produzindo dados a todo instante.

A proteção aos dados pessoais neste contexto passa a ser um elemento fundamental para o desenvolvimento de direitos da personalidade, mais especificamente da intimidade e privacidade, além de evidentes reflexos na autodeterminação do indivíduo na medida em que o controle da própria existência passa pelo controle dos dados pessoais que lhe digam respeito.

A partir da ideia do respeito à privacidade, sendo esta considerada a prerrogativa de não sofrer intromissão de nenhuma pessoa e sob nenhuma forma, o entendimento de que a proteção dos dados pessoais é um direito fundamental é conceito pacífico (MALDONADO;

[3] "Latência significa o tempo que separa um fato acontecido, com os seus dados e o registro e processamento dele." (BARBIERI: 2019, p. 12).

BLUM, 2018, p. 90). Assim, se no início a proteção dos dados pessoais estava compreendida no escopo da proteção à privacidade, na quadra atual esse direito assumiu o caráter de direito autônomo, uma decorrência natural da evolução tecnológica e da importância que os dados e informações assumiram no contexto econômico e social da sociedade líquida.

O indivíduo no contexto do *Big Data*, da IoT e da dataficação encontra-se em evidente posição de desigualdade e vulnerabilidade no que tange à proteção aos dados pessoais. A necessidade de manipulação de dados na sociedade digital, motivada por questões econômicas e a necessidade de geração de novos modelos para negócios expõe um cenário em que a pessoa natural não dispõe de controle sobre seus próprios dados.

Segundo COTS e OLIVEIRA (2019, p. 46), "[...] *dificilmente uma pessoa natural deixaria de se encontrar na posição de fragilidade, pois os dados, por serem na grande maioria dos casos intangíveis, não permite ao titular certeza jurídica de seu tratamento*.", ficando evidente que a posição da pessoa natural é de absoluta vulnerabilidade. Os fenômenos do *Big Data*, do IoT e da dataficação não podem se tornar em justificativas para o tratamento de dados pessoais ao arrepio da lei. O *Big Data* envolve a manipulação de grandes quantidades de dados, o que não implica que esse tratamento somente será possível quando houver a desconsideração de preceitos éticos e jurídicos ligados ao respeito aos dados pessoais.

Inovação tecnológica não é incompatível com o respeito e a proteção aos direitos fundamentais e a ação instrumental não pode produzir avanços científicos que venham a mitigar qualquer direito fundamental. Como ponderou HABERMAS (2004, p. 52):

> Lesões ao direito humano não podem ser reduzidas a infrações às representações axiológicas. A diferença entre direitos, ponderados de maneira fixa, e bens, que podem ser considerados prioritários ou não dependendo de cada nova ponderação, não deveria ser confundida.

No contexto da sociedade da informação, a decisão sobre o uso de dados pessoais deve ser garantida àqueles que são os seus titulares, sob pena de transformar o indivíduo em um objeto do ato de decisão de outrem (SLOTERDIJK, 2000, p. 44), sendo que "*A proteção da pessoa humana deve ser entendida como valor máximo do ordenamento jurídico*" (MALDONADO; BLUM, 2019, p. 48). Ou seja, no cenário do *Big Data*, do IoT e da dataficação "*Todos os indivíduos têm também o direito à proteção de dados, incluindo o controle sobre coleta, retenção, tratamento, eliminação e divulgação de dados pessoais*" (MALDONADO; BLUM, 2019, p. 50).

No âmbito da União Europeia, o artigo 8º da Convenção Europeia dos Direitos do Homem (CEDH) de 1950, em vigor desde 1953, trouxe proteção contra a coleta e manipulação de dados pessoais, reconhecendo que tal proteção integra o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência. Essa proteção aos dados pessoais não era expressa e decorria da proteção à vida privada.

Contudo, foi com a Convenção nº 108, de 1981, que a União Europeia trouxe expressa proteção aos dados pessoais, sendo assim o primeiro instrumento no âmbito internacional a prever a proteção de dados, surgindo em um contexto de crescimento da tecnologia da informação.

O artigo 1º da Convenção nº 108 declara a proteção face ao tratamento automatizado de dados de caráter pessoal, abarcando todo e qualquer tratamento realizado no âmbito público ou privado. Em sintonia com a necessidade de proteção aos dados pessoais, o artigo 17 da LGPD dispõe sobre a titularidade dos dados pessoais, ao prescrever, *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.

Ou seja, a titularidade dos dados pessoais é sempre da pessoa natural, sendo um direito intransmissível e irrenunciável segundo acepção do artigo 11 do Código Civil[4], pois integra o rol de direitos da personalidade (BOTELHO, 2020b, p. 202). Da redação do artigo 17 da LGPD verifica-se que não é possível efetuar uma desvinculação dos dados pessoais da pessoa de seu titular quando houver o tratamento pelo controlador ou operador. Ademais:

> 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. 119.

O escopo da lei não se traduz na caracterização de um direito absoluto. Da leitura do artigo 17 da LGPD verifica-se a possibilidade de restrições e de exceções ao direito albergado na norma quando houve a preponderância de outros interesses à vontade do titular (MALDONADO; BLUM, 2019, p. 221)

2 O TRATAMENTO DE DADOS PESSOAIS PELAS PESSOAS JURÍDICAS DE DIREITO PÚBLICO: FINALIDADE E INTERESSE PÚBLICO

A Lei nº 13.709, de 14 de agosto de 2018 – a chamada Lei Geral de Proteção de Dados Pessoais – surge em um contexto em que a preocupação tanto interna quanto externa com a proteção de dados pessoais é evidente, inserindo o Brasil no grupo de países que dispõem de normas relativas ao tratamento de dados pessoais. Com o escopo de proteger direitos fundamentais da pessoa natural a LGPD visa estabelecer regras que permitam um tratamento de dados pessoais em conformidade com as normas que impõe respeito à pessoa humana. No

[4] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária

Brasil,

> [...] na atualidade, a LGPD assume o papel de principal legislação existente sobre o tema, incluindo o estabelecimento de fundamentos e princípios que transpassam a própria lei, norteando e aclarando o pensamento jurídico (COTS; OLIVEIRA, 2019, p. 19).

Consoante prevê o artigo 1º, parágrafo único da LGPD as normas gerais contidas na Lei nº 13.709, de 2018 são de interesse nacional e de observância obrigatória pelos entes federativos. O próprio *caput* do artigo em questão é explícito ao declarar que entre os destinatários da norma está a pessoa jurídica de direito público. A expressão "interesse nacional" aponta para a transcendência do plexo de normas presentes na Lei nº 13.1709, de 2018, conferindo-lhe uma posição de destaque no ordenamento jurídico brasileiro, expressando a sua força para disciplinar as relações jurídicas que abarquem o tratamento de dados para além das competências atribuídas a cada ente federativo.

Não significa que a Lei nº 13.709, de 2018 modificou competências constitucionais dos entes federativos ou mitigou o alcance de normas constitucionais neste campo. É preciso lembrar que a proteção aos dados pessoais é um direito da personalidade, estando na esfera de competência privativa da União (art. 22, inciso I) a produção legislativa. Neste contexto, Estados, Municípios e o Distrito Federal não podem criar uma panaceia legislativa, produzindo normas que se distanciem das bases e princípios postos na LGPD a fim de disciplinar a proteção de dados pessoais.

A proteção aos dados pessoais tem como premissas não apenas as normas elencadas na Constituição Federal acerca dos direitos da personalidade, mas agora, também, os princípios e normas tratados na Lei nº 13.709, de 2018, de modo que não há impedimento à capacidade legislativa dos entes federativos (MALDONADO; BLUM, 2019, p. 24), mas apenas o estabelecimento de parâmetros gerais de observância obrigatória por todos os entes da

federação. E a lógica da expressa inclusão dos entes públicos como destinatários da Lei nº 13.709, de 2018 é clara: o poder público efetua tratamento de dados pessoais.

Ademais, a importância do tema veio à tona por ocasião do julgamento pelo Supremo Tribunal Federal da constitucionalidade da Medida Provisória nº 954, de 17 de abril de 2020, que dispôs sobre o compartilhamento de dados pessoais, como nomes, números de telefone e endereços de seus consumidores, por empresas de telecomunicações prestadores de serviços de telefonia com o IBGE[5], sobretudo porque a Corte Maior aplicou ao caso normas da LGPD mesmo antes de sua entrada em vigor, conforme pode ser extraído de trecho da decisão liminar proferida pela Ministra Rosa Weber:

> [...] o respeito à privacidade e à autodeterminação informativa foram positivados, no artigo 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

Bancos de dados com informações pessoais de cidadãos são largamente utilizados pelos entes federativos, muitas vezes sem a implementação de boas práticas em segurança da informação, sem medidas que protejam os dados de inúmeros cidadãos.

> É inerente à atividade administrativa a gestão de uma série de bancos de dados potencialmente sensíveis, sendo que a coleta e tratamento desses dados é um ponto nevrálgico em termos de políticas públicas que tenham escala (MALDONADO; BLUM, 2019, p. 246.

A segurança da informação tem por desiderato a garantia da integridade, confidencialidade, autenticidade e disponibilidade das informações que são tratadas por

[5] STF, ADIn 6387

determinada organização, as quais devem ter políticas de segurança da informação (PSI), entendida como um plexo de princípios que nortearão a gestão da segurança da informação.

A LGPD traz normas específicas ao tratamento de dados pessoais pelo poder público nos artigos 23 a 30, dada a relevância da atuação dos entes públicos na coleta e manipulação de dados pessoais. Logo, "*Por estar atrelado à lei, o Poder Público precisa das permissões legais adequadas para sua atuação, o que inclui a possiblidade de tratamento de dados de pessoas naturais, como prevê a LGPD*" (COTS; OLIVEIRA, 2019, p. 137). Desta forma, o *caput* do artigo 23 da LGPD traz a seguinte norma, *in verbis*:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

O dispositivo menciona as pessoas jurídicas de direito público referidas no parágrafo único do artigo 1º da Lei de Acesso à Informação. Este dispositivo assevera que estão subordinadas à Lei de Acesso à Informação e, por conseguinte, à LGPD, os órgãos públicos integrantes da administração direta dos Poderes, abarcando, também, as Cortes de Contas e o Ministério Público, bem como as autarquias, fundações públicas, empresas públicas, as sociedades de economia mista e todas as demais entidades que sejam controladas direta ou indiretamente por qualquer dos entes federativos. Acrescente-se a este rol os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, conforme prescreve o § 4º do artigo 23 da LGPD.

Quanto às empresas públicas e as sociedades de economia mista que atuam em regime de concorrência e que estão sujeitas ao imperativo do artigo 173 da Constituição Federal, o

artigo 24 da LGPD é expresso em afirmar que terão elas o mesmo tratamento que é dispensando às pessoas jurídica de direito privado. Excetua-se esta regra nos casos em que as empresas públicas e as sociedades de economia mista estiverem operacionalizando políticas públicas quando, no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e entidades do Poder Público. Qualquer coleta e tratamento de dados pessoais deve ser levado à cabo para atendimento de finalidade pública. A finalidade evoca a noção de consequência (JUSTEN FILHO, 2011, p. 371) que, no caso do poder público, deve ser pública, pois "[...] *a finalidade pública diz respeito ao chamado interesse público primário*". (AMARAL, 2020, p. 87)

Logo, a finalidade será pública se o interesse também for público (COTS; OLIVEIRA, 2019, p. 138), impondo ao poder público o dever se buscar objetivos que se traduzam na promoção do interesse público. Segundo JUSTEN FILHO (2011, p. 372):

> A vinculação normativa quanto às finalidades restringe-se a determinar que nenhum fim privado ou alheio ao bem da coletividade pode ser perseguido por meio das competências estatais. [...] Quando exercita uma função estatal, o agente promove a concretização do ordenamento jurídico em seu conjunto. Logo, existem inúmeras finalidades a serem realizadas. É indispensável identificar essas finalidades contempladas de modo teórico no ordenamento jurídico.

A finalidade deve ser entendida como a efetivação de qualquer tratamento de dados pessoais em conformidade com objetivos legítimos, específicos, explícitos e informados ao titular, vedando-se qualquer tratamento posterior que esteja em descompasso com tais finalidades. Logo, considerando o regime jurídico próprio do direito administrativo, um tratamento levado a cabo sem observância do princípio da finalidade caracteriza o chamado desvio de finalidade (AMARAL, 2020, p. 83).

O conceito legal de desvio de finalidade vem previsto no artigo 2º, parágrafo único, letra *e* da Lei nº 4.717, de 29 de junho de 1965, que prescreve, *in verbis*:

> Art. 2º *Omissis*. [...]
>
> e) o desvio de finalidade se verifica quando o agente pratica o ato visando a fim diverso daquele previsto, explícita ou implicitamente, na regra de competência.

A regra de competência é outorgada pelas normas da LGPD e são de observância obrigatória pelo Poder Público, demandando do administrador a prática de ato em conformidade com a norma legal e para o atendimento da finalidade nela posta. O artigo 2º da Lei nº 4.717, de 1965 cita, inclusive, que o desvio de finalidade figura como um ato lesivo ao patrimônio dos entes públicos, caracterizando ato de improbidade administrativa.

Segundo AMARAL (2020, p. 84), ao comentar o *caput* do artigo 23 da LGPD:

> A questão disciplinada no preceito legal em apreço reside na finalidade ligada ao interesse público, no exercício de atribuições legais e, evidentemente, resguardadas a adequação e a necessidade do referido tratamento.

Portanto, no âmbito de incidência da LGPD, a finalidade pública será observada nos casos em que o Poder Público proceder ao tratamento de dados pessoais dos administrados atendendo aos estritos termos legais no que tange à formulação e execução de políticas públicas, havendo, em razão disso, a necessidade de implementar as medidas aptas à proteção de dados da pessoa natural.

O uso de dados pela Administração Pública com vistas à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres figura como uma das bases legais para o tratamento de dados pessoais. E mesmo

os dados pessoais cujo acesso seja público não estão dispensados, em seu tratamento, da observância da finalidade, boa-fé e o interesse público que justificaram a sua disponibilização[6]. Assim, o tratamento de dados pessoais deve se pautar pela persecução do interesse público, que não deve ser confundido com interesse estatal. Segundo JUSTEN FILHO (2011, p. 120):

> Em um Estado Democrático de Direito, o Estado somente está legitimado a ser sujeito de interesses públicos, assim entendidos como aqueles direta e imediatamente relacionados com os direitos fundamentais.

Embora haja uma certa indeterminação do conceito de interesse público, há diversos graus de indeterminação e nem sempre a ideia terá um sentido indeterminado (DI PIETRO, 2004, p. 72). Primeiramente, há que se considerar que no contexto da proteção aos dados pessoais, o interesse público jamais pode representar no acolhimento de atos produzidos pela Administração Pública que venham a causar ofensa aos direitos fundamentais ou a mitigação da dignidade da pessoa humana.

A busca pela satisfação do interesse público revela a razão de ser do Estado, sendo que, considerando a ideia de interesse primário, expressa a noção de que a promoção da justiça, segurança e bem-estar estão na base dessa existência (MULHOLLAND; MATERA, 2020, p. 223). Desta maneira, qualquer tratamento de dados pessoais levado a cabo pelas pessoas jurídicas de direito público deve promover a justiça, a segurança e o bem-estar, sob pena de estar em desconformidade com a LGPD.

Embora não seja exigido do Poder Público a obtenção do consentimento do titular dos dados para o tratamento de dados pessoais nos casos em que for necessário para a execução

[6] Artigo 7º, § 3º, da LGPD.

de políticas públicas previstas em lei ou regulamentos (TERRA; CASTRO, 2020, p. 249), não significa que o tratamento não tenha que ser feito em observância aos princípios que regem a administração pública. Logo:

> Na esteira dos princípios que regem a atuação da Administração Pública previstos no artigo 37 da Constituição da República, quais sejam, legalidade, impessoalidade, moralidade, publicidade e eficiência, o artigo 23 da LGPD demanda que o tratamento de dados pessoais pelo estado observe a finalidade e o interesse públicos, tendo como objetivo a execução das competências e a prestação dos serviços públicos nos termos da Lei (TERRA; CASTRO, 2020, p. 249).

A execução das competências legais ou cumprimento das atribuições legais do serviço público expressa a necessidade de que o tratamento deve ter o princípio da legalidade subjacente. Desta maneira, o tratamento a ser realizado pelas pessoas jurídicas de direito público deve estar circunscrito no âmbito de suas competências constitucionais e legais, impondo, ainda, a necessidade de informação das hipóteses em que o tratamento de dados pessoais é realizado, sendo que tal informação deve ser clara e atualizada sobre a previsão normativa, qual a finalidade, os procedimentos e as práticas utilizadas para a execução dessa atividade, disponibilizada em veículos de fácil acesso, preferencialmente nos sítios eletrônicos oficiais. Destarte, como escreve AMARAL (2020, p. 78):

> O Poder Público, pela própria essência do direito constitucional, não pode violar a privacidade de indivíduos, salvo nas hipóteses legalmente admitidas, quando então se fará presente como fator para tal autorização o interesse público.

A pessoa jurídica de direito público haverá de indicar, ainda, um encarregado quando

houver o tratamento de dados pessoais, conforme norma plasmada no artigo 23, inciso III da LGPD. Significa que, além da observância da base principiológica e normativa aplicável a atuação da Administração Pública, o tratamento de dados pessoais somente poderá ser realizado quando houver a indicação de um encarregado (*Data Protection Officer - DPO*).

Segundo a LGPD, o *DPO* deve servir como ponto de contato entre o controlador, a Autoridade Nacional de Proteção de Dados e o titular de dados, cabendo-lhe, segundo o artigo 41, § 2º da LGPD, aceitar as reclamações e comunicações dos titulares, além de prestar esclarecimentos e adotar providências, receber comunicações provenientes da ANPD e adotar providências, proceder a orientação dos funcionários e dos contratados da entidade acerca das práticas a serem tomadas em relação à proteção de dados pessoais, e executar as demais atribuições que forem determinadas pelo controlador ou que estejam estabelecidas em normas complementares (BOTELHO, 2020b, p. 204).

Segue-se, ademais, que o DPO deve efetivar um monitoramento permanente da conformidade com a LGPD, procedendo uma constante avaliação quanto a realização das atividades de tratamento de dados pessoais em conformidade com os princípios e regras constantes da LGPD. Importante destacar que o agente de tratamento tem o dever legal de adotar medidas que sejam reputadas eficazes e aptas para comprovar que houve a observância das normas de proteção de dados pessoais, inclusive no tocante a eficácia das medidas (AMARAL, 2020, p. 87). Ou seja, como corolário do princípio da eficiência, estampado no *caput* do artigo 37 da Constituição Federal, as medidas implementadas pelo Poder Público devem possuir efetividade e garantir a proteção dos dados pessoais, pois:

> Exige-se de todo aquele que trata de dados pessoais, inclusive do Poder Público, para efetivar os princípios e consolidar os fundamentos legais, a manutenção de mecanismos por meio dos quais viabilize o acesso correto aos dados pelos titulares, bem como a finalidade do tratamento informado (AMARAL, 2020, p. 87).

Essa exigência de proteção aos dados pessoais ocorre sobre todo o ciclo de vida dos dados (BOTELHO, 2020a, p. 212), ou seja, desde a sua coleta até o descarte dos dados a observância de boas práticas em segurança da informação devem estar presentes. O artigo 23, § 1º da LGPD prescreve, ademais, que a ANPD poderá dispor sobre as formas de publicidade das operações de tratamento de dados pessoais pelo Poder Público. Este dispositivo deixa patente a necessidade de transparência nas operações de tratamento de dados pessoais pelo Poder Público.

A ANPD tem a competência de zelar pela proteção dos dados pessoais, além de dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, solicitar às entidades do Poder Público que efetuem a realização de operações de tratamento de dados pessoais, que confeccionem informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, bem como comunicar aos órgãos de controle interno eventual descumprimento da normas da LGPD. Essa necessidade de transparência, como corolário do princípio da publicidade plasmado no *caput* do artigo 37 da Constituição Federal (MALDONADO; BLUM, 2019, p.

263) é claramente percebida pela leitura da redação do § 2º do artigo 23, o qual assevera que a observância da LGPD não dispensa o Poder Público de instituir as autoridades elencadas na Lei de Acesso à Informação (LAI). Dúvidas poderiam surgir com relação a possíveis conflitos que poderiam surgir na atuação do encarregado (DPO) previsto na LGPD e a autoridade responsável pela custódia da informação na Lei de Acesso à Informação.

A interpretação dos papéis definidos pela LGPD e pela LAI deve buscar harmonizar as atribuições legais previstas de modo a promover a maior eficácia possível da publicidade e da proteção de dados pessoais. Assim, a disciplina acerca da existência de uma autoridade com atribuições de cumprir as normas da LAI, sobretudo de prestar informações ao cidadão, não significa a dispensa da obrigação quanto à instituição de um encarregado nos termos da

LGPD (MALDONADO; BLUM, 2019, p. 262). Desta maneira,

> Enquanto a autoridade de acesso à informação tem por investidura legal dar acesso ao cidadão a toda informação passível de publicidade sob custódia da Administração Pública, observada a matriz de sigilo, ao encarregado cabe, entre outras atribuições, justamente o oposto, qual seja a preservação de dados pessoais e dados sensíveis que estejam em bases públicas (MALDONADO; BLUM, 2019, p. 262).

Aqui é importante compreender-se que a informação tutelada pela LAI é aquela considerada pública ou abrangida pelo interesse público, razão por que, trata-se de informação que pertence à coletividade e que deve estar disponível ao cidadão. Diferente é a tutela ofertada pela LGPD, que abarca os dados considerados pessoais, relacionados à pessoa natural identificada ou identificável.

O propósito da LAI não é mitigar a proteção à privacidade, à intimidade e aos dados pessoais, havendo norma expressa no inciso III do artigo 6º que impõe o dever do Poder Público de proteger a informação pessoal, considerada aquela relacionada à pessoa natural identificada ou identificável (art. 4º, inciso IV da LAI). Ou seja, "*Tais dados não podem ser de conhecimento da sociedade, somente aqueles que estejam em uma zona de plena publicidade, para os quais, neste caso, seria vedado qualquer tipo de sigilo*" (HEINEN, 2015, p. 133)

Ademais, conforme afirma SALGADO (2015, p. 97):

> A existência da regra da publicidade e da transparência não promove de imediato o amplo acesso a qualquer informação, tendo em vista outros bens jurídicos protegidos pela Constituição e pelo ordenamento.

Portanto, as figuras do encarregado da LGPD e da autoridade de que trata a LAI são

complementares e obrigatórias as suas instituições pelo Poder Público, cujo descumprimento gera efeitos deletérios para o exercício dos direitos fundamentais tutelados nos diplomas normativos em questão, sendo passível de caracterização da prática de improbidade administrativa pelo gestor público.

3 DA INTEROPERABILIDADE E DO COMPARTILHAMENTO DE DADOS PELO PODER PÚBLICO

O compartilhamento de dados é possibilitado pela LGPD em situações que especifica, devendo-se entender, contudo, o que significa a expressão "uso compartilhado de dados", cuja definição legal encontra-se no inciso XVI do artigo 5º da Lei, *in verbis*:

> Art. 5º *Omissis*. [...]
>
> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Nota-se que no conceito de uso compartilhado de dados, há a expressa menção ao compartilhamento feito por órgãos e entidades públicos no cumprimento de suas competências legais, bem como o compartilhamento levado a cabo entre o Poder Público e entes privados. Para que haja o compartilhamento pelo Poder Público, a LGPD exige que os dados estejam em formato interoperável e estruturado para o uso compartilhado, para os fins de execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Interoperabilidade expressa a ideia de que os sistemas e organizações possuam a capacidade de trabalharem em conjunto de maneira a possibilitar que pessoas, organizações e sistemas computacionais estejam aptos a proceder o intercâmbio de informações de forma eficaz e eficiente (MALDONADO; BLUM, 2019, p. 269). Assim, a interoperabilidade indica a preocupação com o intercâmbio entre sistemas, processos e culturas, gerenciados de uma maneira que promova a maximização das oportunidades e a reutilização de informações (UKOLN, 2005).

No âmbito da tecnologia da informação, a interoperabilidade engloba a ideia da capacidade dos computadores e programas de distintos fabricantes trocarem informações, abarcando seis áreas descritas por SAYÃO e MARCONDES (2008, p. 136), a saber, a interoperabilidade técnica, a interoperabilidade semântica, a interoperabilidade política/humana, a interoperabilidade intercomunitária, a interoperabilidade legal e a interoperabilidade internacional.

A interoperabilidade técnica leva em conta os aspectos técnicos com vistas desenvolver padrões de comunicação, transporte, armazenamento e representação das informações, abarcando, ainda, esforços para que padrões individuais venham a evoluir em benefício da comunidade, objetivando uma convergência de padrões. A interoperabilidade semântica liga-se ao significado das informações provenientes de distintos recursos, impondo a adoção de soluções que perpassem pela utilização de ferramentas comuns de representação da informação.

A interoperabilidade política/humana envolve as decisões que tornam as informações e recursos disponíveis da maneira mais ampla e interoperável, trazendo consequências para a organização, para as equipes envolvidas e para os usuários no campo comportamental, de recursos e de treinamento. Quando se fala de uso compartilhado de dados pelo Poder Público, a interoperabilidade política/humana significa que:

> A ênfase dada por parte de alguns setores governamentais aos

> problemas de democratização do acesso, da inclusão digital e da federação de fontes de informação voltadas para a educação a distância, tem impacto nas políticas públicas para a área (SAYÃO; MARCONDES, 2008, p. 137).

A interoperabilidade intercomunitária decorre no aumento da necessidade do acesso à informação a uma ampla gama de fontes, o que demanda a criação de fóruns de discussão e consenso em torno de práticas e procedimentos comuns. As exigências e consequências legais de promover a disponibilidade da informação entra na ideia de interoperabilidade legal.

Por fim, a interoperabilidade internacional demanda esforços com vistas a solucionar questões envolvendo a diversidade de padrões e normas, problemas de comunicação, barreiras linguísticas, estilos de comunicação distintos e ausência de uma fundamentação comum. Desta maneira, a exigência contida no artigo 25 da LGPD é que o dado possa ser objeto de tratamento por qualquer sistema e esteja apto a transitar pela *web*, impondo-se dados em padrão aberto e "[...] *que sistemas que vão trabalha-lo estejam aptos a fazê-lo, independentemente do fato de também adotarem a concepção de código aberto*". (MALDONADO; BLUM, 2019, p. 270).

Importa salientar que a exigência contida no artigo 25 da LGPD é de que os dados deverão ser armazenados em formato aberto, pois não será possível a interoperabilidade nos casos de armazenamento em formato fechado. Esse formato aberto não pode ser confundido com o conceito de dados abertos e que, no Brasil, está disciplinado no Decreto nº 8.777, de 11 de maio de 2016, que instituiu a política de dados abertos no Poder Executivo Federal.

O Decreto nº 8.777, de 2016 traz a definição do que seja "formato aberto" no artigo 2º, inciso IV, *in verbis*:

> Art. 2º *Omissis*.

> [...]
> IV - formato aberto - formato de arquivo não proprietário, cuja especificação esteja documentada publicamente e seja de livre conhecimento e implementação, livre de patentes ou qualquer outra restrição legal quanto à sua utilização.

AMARAL (2020, p. 89) lembra que a existência de bases distintas e que não sejam interoperáveis traz prejuízos à eficiência na execução de suas competências pelo Poder Público, além de representar um aumento injustificável do risco de ocorrência de incidentes com dados pessoais. O compartilhamento de dados pessoais pelo Poder Público vem disciplinado no artigo 26 da LGPD. Segundo o *caput* deste dispositivo, o atendimento de finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas são requisitos para que possa haver o uso compartilhado de dados pessoais, sempre respeitados os princípios de proteção estampados no artigo 6º da LGPD.

Esse compartilhamento de dados pessoais é somente no âmbito da Administração Pública, evidenciando-se na LGPD a necessidade de uma finalidade pública específica para que seja realizado o uso compartilhado de dados pessoais (FEIGELSON; SIQUEIRA, 2019, p. 142). Assim, o § 1º do artigo 26 da LGPD traz como regra a vedação da transferência à entidades privadas de dados pessoais constantes de base de dados que o Poder Público tenha acesso, prevendo, contudo, quatro exceções.

A primeira exceção diz respeito aos casos de execução descentralizada de atividade pública que demande a transferência, exclusivamente para esse fim determinado e específico, não sendo "[...] *permitido o compartilhamento de dados desnecessários para as finalidades pretendidas*". (COTS; OLIVEIRA, 2019, p. 148). Em outras palavras, somente a execução de atividade pública é que figurará como o único fator legitimador para a transferência de dados, vedando-se qualquer desvio da finalidade pública, com a extensão da transferência

delimitada pelo princípio da necessidade que impõe o dever de transferir somente os dados que são necessários para a execução da atividade pública (MALDONADO; BLUM, 2019, p. 282).

A segunda exceção refere-se aos casos em que os dados forem acessíveis publicamente, observadas as disposições da LGPD. Aqui é importante destacar que essa exceção deve ser interpretada em conjunto com o artigo 17 da LGPD que assegura a titularidade à pessoa natural de seus dados pessoais, além de garantir os direitos fundamentais de liberdade, de intimidade e de privacidade. Também deve ser levado em conta o disposto no § 3º do artigo 7º da LGPD que assevera que o tratamento de dados pessoais cujo acesso seja público deve considerar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização. Desta forma:

> A regra de contenção [...] preconiza que, ainda que acessíveis publicamente, o fundamento de validade do ato de transferência deve advir do sucesso do Teste de Proporcionalidade para aferição, sobretudo, do atendimento ao princípio da boa-fé e da finalidade (MALDONADO; BLUM, 2019, p. 282).

Isso significa que a acessibilidade pública aos dados pessoais não significa carta branca para a sua transferência a entidade privada sem que a finalidade pública esteja subjacente à prática deste ato. A terceira exceção ocorre quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres. Esta hipótese de afastamento da regra de vedação da transferência é objeto de críticas na medida em que pode levar à conclusão equivocada de que o Poder Público poderia efetuar a transferência com respaldo em documento legal, contrato, convênio ou instrumento congênere (MALDONADO; BLUM, 2019, p. 282).

COTS e OLIVEIRA (2019, p. 148) advertem que tanto a previsão legal quanto os

contratos, convênios ou instrumentos congêneres deverão estar respaldados pela LGPD, não podendo, em hipótese alguma, ir de encontro ao que ela prevê, principalmente no tocante aos seus fundamentos. Outrossim:

> [...] não se sustenta a mera existência de previsão legal ou contratual se não amparada no sucesso em superar o Teste de Proporcionalidade, baseado nos princípios de proteção de dados do artigo 6º (MALDONADO; BLUM, 2019, p. 283).

Ademais, por força da norma plasmada no § 2º do artigo 26 da LGPD, os contratos e convênios a que se refere a exceção em comento deverão ser comunicados à ANPD. A última exceção prevista diz respeito a hipótese de transferência visando exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular de dados, desde que vedado o tratamento para outras finalidades.

Esta hipótese é ampla (COTS; OLIVEIRA, 2019, p. 143 / MALDONADO; BLUM, 2019, p. 283), exigindo-se cautela na sua aplicação, a fim de evitar a exposição indevida de dados pessoais a terceiros sob a justificativa de protege-los. É importante lembrar que os agentes de tratamento devem implementar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais (art. 46 da LGPD), o que impõe a responsabilidade no manejo desses dados, principalmente no que se refere ao seu compartilhamento com pessoas de direito privado.

O artigo 27 da LGPD disciplina os casos de comunicação, difusão, interconexão e tratamento compartilhado, diferentemente do que ocorre no § 1º do artigo 26 que se refere à transferência. Há, porém, uma impropriedade redacional, na medida em que o artigo 27 da LGPD fala em "comunicação" e no "uso compartilhado" como sendo hipóteses distintas. Contudo, o artigo 5º, inciso XVI da LGPD dispõe que a comunicação é uma espécie de uso compartilhado.

Segundo a redação do artigo 27, a comunicação, difusão, interconexão e tratamento compartilhado de dados pelo Poder Público à pessoa de direito privado deverão ser informados à ANPD e dependerá de consentimento do titular. Ou seja, a regra é a necessidade do consentimento para que essas hipóteses de uso compartilhado de dados possam ser efetivadas (MALDONADO; BLUM, 2019, p. 285), havendo, porém, a previsão de exceções, disciplinadas em três incisos do artigo 27, a saber, nas hipóteses de dispensa de consentimento previstas na LGPD, nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do artigo 23, inciso I da LGPD ou, ainda, nas exceções previstas no § 1º do artigo 26.

Destaque-se que, por força do artigo 29 da LGPD, a ANPD poderá solicitar, a qualquer momento, ao Poder Público a realização de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados, bem como outros detalhes do tratamento realizado, podendo, ademais, emitir parecer técnico complementar com vistas à garantir o cumprimento da LGPD. Pode, ainda, estabelecer normas complementares para as atividades de comunicação e uso compartilhado de dados pessoais. Assim, o artigo 30 da LGPD expressa o poder normativo da ANPD, em consonância com os artigos 11, §3º e 55-J, inciso II que trazem normas atinentes à atividade regulatória da ANPD.

CONSIDERAÇÕES FINAIS

Vivemos na sociedade da informação, cercados por dispositivos que captam nossos passos e que manipulam nossos dados pessoais, sobre os quais não temos controle, na maioria das vezes.

Neste mundo das relações eletronicamente mediadas (BAUMAN, 2013, p. 21), em que princípios panópticos são uma realidade que não se pode negar, a pessoa natural encontra-se em relação de desvantagem e vulnerabilidade.

Não temos o controle sobre nossos dados pessoais, sobre quem os coleta, sobre o uso

que fazem deles, embora soframos as consequências da exposição e violação da nossa liberdade e privacidade. Segundo o jornalista americano Andrew Lewis, na nova economia de dados, "*Se você não está pagando pelo produto, você é o produto*" (*apud* NASCIMENTO, 2019, p. 17), expondo a reificação do sujeito nas relações produzidas pela sociedade da informação.

É neste contexto de patente vulnerabilidade do titular dos dados que a LGPD surge como norma protetiva de direitos fundamentais de significativa importância para a pessoa natural, positivando de forma explícita acerca da titularidade dos dados e as bases legais que poderão justificar o uso de dados pessoais por terceiros.O Poder Público surge neste quadro como maior detentor de informações e dados pessoais, e casos recentes, como a tentativa da Via Quatro, concessionária da Linha 4 – Amarela do metrô em São Paulo de coletar dados de som e imagem dos usuários através de câmeras instaladas nas estações, e as disposições da Medida Provisória nº 954, de 17 de abril de 2020, que permitiam que o IBGE compartilhasse dados de usuários de telefonia, deixam patente a necessidade de normas voltadas à atuação do Poder Público na realização de tratamento de dados pessoais.

O legislador, sensível a este problema, fez constar na LGPD um capítulo destinado a disciplina do tratamento de dados pessoais pelo Poder Público. Esta disciplina, como visto, deve levar em conta os fundamentos e princípios previstos na LGPD, além dos princípios que informam a Administração Pública e previstos na Constituição Federal. Além disso, a finalidade pública e o interesse público são fundamentais para que o tratamento de dados pessoais pelo Poder Público seja legítimo e esteja em conformidade com a LGPD.

O Poder Público, portanto, somente poderá tratar dados pessoais desde que presentes a finalidade pública e o interesse público, não se admitindo qualquer invasão à privacidade que não esteja justificado a partir de objetivos relacionados à execução de políticas públicas.

Qualquer medida que não respeite a autodeterminação informativa, não permitindo que o titular de dados possa acompanhar o que é realizado com seus dados pessoais não é

tolerada pela LGPD, tornando ilegais as coletas como a pretendida pela Via Quatro. Também o compartilhamento de dados pelo Poder Público com pessoa jurídica de direito privado somente se justifica nos casos em que a finalidade pública e o interesse público estejam presentes, mesmo nos casos de banco de dados de acesso público.

Eventuais violações as normas da LGPD devem receber a devida punição, podendo caracterizar atos de improbidade administrativa, cabendo ao Ministério Público e a própria sociedade civil fiscalizar os atos praticados pelo administrador público quanto a sua conformidade com a LGPD.

REFERÊNCIAS

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

AMARAL, Luiz Fernando de Camargo Prudente do. Desafios da LGPD em relação à implementação pelo poder público. In: BLUM, Renato Opice (org.). *Proteção de dados: desafios e soluções na adequação à lei*. Rio de Janeiro: Forense, p. 77-92, 2020.

BARBIERI, Carlos. *Governança de dados: práticas, conceitos e novos caminhos*. Rio de Janeiro: Alta Books, 2019.

BAUMAN, Zygmunt. *Vigilância líquida*. Rio de Janeiro: Zahar, 2013.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. Bebedouro: *Revista Direitos Sociais e Políticas Públicas*. Unifafibe. Vol. 8, Nº 2, p. 197-231, 2020a.

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a lei Geral de Proteção de Dados Pessoais. Jacarezinho: *Argumenta Journal Law*. UENP. Nº 32, jan./jul., p. 191-207, 2020b.

BOTELHO, Marcos César; CAMARGO, Elimei P.A. A aplicação da lei geral de proteção de dados na saúde. São Paulo: Revista de Direito Sanitário, v. 21, p. 1-21, 2021.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de dados pessoais comentada*. 2. ed.

São Paulo: Revista dos Tribunais, 2019.

DI PIETRO, Maria Sylvia. O princípio da supremacia do interesse público: sobrevivência diante das ideias do neoliberalismo. São Paulo: *Revista Direito Público*. Nº 48, Malheiros, p. 63-76, 2004.

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.

GROHMANN, Rafael. Financeirização, midiatização e dataficação como sínteses sociais. Montevideo: *Mediaciones de la Comunicación*. Universidad Ort. Vol. 14, Nº 2, p. 97-117, 2019.

HABERMAS, Jürgen. *O futuro da natureza humana*. São Paulo: Martins Fontes, 2004.

HAN, Byung-Chul. *No enxame: perspectivas do digital*. Petrópolis: Vozes, 2018.

HEINEN, Juliano. *Comentários à lei de acesso à informação: Lei nº 12.527/2011*. 2. ed. Belo Horizonte: Editora Fórum, 2015.

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

JUSTEN FILHO, Marçal. *Curso de direito administrativo*. 7. ed. Belo Horizonte: Editora Fórum, 2011.

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

KRELL, Andreas Joachim; SILVA, Carlos Henrique Gomes da. Por uma concepção neoconstitucional da cidadania: da cidadania política à cidadania social e jurídica. *Revista Direitos Sociais e Políticas Públicas – Unifafibe*. V. 9, N. 1, 2021.

MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords). *LGPD: Lei geral de proteção de dados comentada*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

MANGO, Cynthia Ferrari. Gestionando la política social territorialmente: el "Argentina trabaja" desde el "movimiento evita" (2009 -2018). *Revista Direitos Sociais e Políticas Públicas – Unifafibe.* V. 9, N. 1, 2021.

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

MORALES, Julio César Arellano. Derecho al libre desarrollo de la personalidad. *Revista Direitos Sociais e Políticas Públicas – Unifafibe.* V. 9, N. 1, 2021.

MULHOLLAND, Caitlin; MATERA, Vinicius. O tratamento de dados pessoais pelo poder público. In: MULHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago editoral, p. 217-236, 2020.

NASCIMENTO, Rodrigo. *Marketing na era dos dados: o fim do achismo*. São Paulo: Évora, 2019.

SALGADO, Eneidad Desiree. *Lei de acesso à informação (LAI): comentários à Lei nº 12.527/2011 e ao Decreto nº 7.724/2012.* São Paulo: Atlas, 2015.

SAYÃO, Luis Fernando; MARCONDES, Carlos Henrique. O desafio da interoperabilidade e as novas perspectivas para bibliotecas digitais. Campinas: *TransInformação*. 20(2), mai./ago., p. 133-148, 2008.

SAWAYA, Márcia Regina. *Dicionário de informática & internet inglês/português.* São Paulo: Nobel, 1999.

SCHUTT, Rachel; O'NEIL, Cathy. *Doing data Science*. Sebastopol: 2014.

SIQUEIRA, Dirceu Pereira; LARA, Fernanda Corrêa Pavesi; SOUZA, Bruna Carolina de. Os direitos humanos e a proteção aos seus defensores: análise à luz da salvaguarda dos direitos de personalidade. *Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)* - ISSN 2318-5732 - v. 8, n. 3, 2020, p. 159-180.

SIQUEIRA, Dirceu Pereira; FERREIRA; ANDRECIOLI, Sabrina Medina. Direitos personalidade das mulheres sob a perspectiva da dignidade da pessoa humana como axioma justificante. *Revista*

Direitos Humanos e Democracia. Programa de Pós-Graduação Stricto Sensu em Direito da Unijuí. Mestrado em Direitos Humanos, 8, n. 15, p. 290-307, 2020.

SIQUEIRA, Dirceu Pereira; ALMEIDA, Fernando Rodrigues de. A impossibilidade de racionalidade dos direitos da personalidade sem um purismo metodológico: uma crítica a partir do debate entre Kelsen e Schmitt. *Revista de Brasileira de Direito (IMED)*, v. 16, n. 1, p. 1 - 27, 2020.

SIQUEIRA, Dirceu Pereira; CASTRO, Lorenna Roberta Barbosa. Minoria feminina e constituições republicanas brasileiras: análise de 1891 a 1988 pela inclusão das mulheres. *Argumenta Journal Law - UENP (Jacarezinho)*, vol. 33, n. 1, p. 361-382, 2020.

TERRA, Aline de Miranda Valverde; CASTRO, Diana Paiva de. A responsabilidade do poder público no tratamento de dados pessoais: análise dos artigos 31 e 32 da LGPD. In: MULHOLLAND, Caitlin (org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago editoral, p. 237-264, 2020.

UKOLN. *Interoperability focus: lookint at interoperatility*. 2005. Disponível em: <http://www.ukoln.ac.uk/interop-focus/about/leaflet.html>. Acesso em: 10.10.2020.

ZAMBAM, Neuro José; SILVEIRA, Margarete Magda da. Projeto renda mínima de cidadania: solução para equidade social. *Revista Direitos Sociais e Políticas Públicas – Unifafibe.* V. 9, N. 1, 2021.

ZANINI, Leonardo Estevam de Assis; QUEIROZ, Odete Novais Carneiro Queiroz. A autonomia privada na aceitação e na renúncia da herança. *Revista Direitos Sociais e Políticas Públicas – Unifafibe.* V. 9, N. 1, 2021.