DOI 10.5433/21788189.2022v26n1p105

INSTRUMENTOS PROCESSUAIS DE PROTEÇÃO DE DADOS

PROCEDURAL INSTRUMENTS OF DATA PROTECTION

Deny Eduardo Pereira Alves*
Adalberto Simão Filho**
Diógenes Faria de Carvalho***

Como citar: ALVES, Deny Eduardo Pereira; FILHO, Adalberto Simão. CARVALHO, Diógenes Faria de. Instrumentos Processuais de Proteção de Dados. **Scientia Iuris**, Londrina, v. 26, n. 1, p. 105-125, mar. 2022. DOI: 10.5433/21788189.2022v26n1p105. ISSN: 2178-8189.

Resumo: O advento da Lei Geral de Proteção de Dados (LGPD) no ordenamento jurídico brasileiro trouxe avanços com relação à tutela, individual e coletiva, dos dados pessoais. O texto normativo contempla, além do direito material, alguns aspectos processuais para a efetivação dos direitos nela previstos. Pretende este trabalho efetuar uma análise desses instrumentos previstos na LGPD, bem ainda estabelecer um diálogo de fontes com os demais diplomas processuais existentes, indicando as potencialidades e dificuldades na tutela dos dados sob proteção.

Palavras-chave: instrumentos processuais, LGPD, proteção de dados, tutela coletiva, tutela individual.

Abstract: The advent of the Data Protection Act (LGPD) in the Brazilian legal system brought advances with regard to legal protection, individual and collective, of personal data. This normative text includes, in addition to civil law, some procedural aspects for the implementation of the rights provided for therein. This study intends to carry out an analysis of these instruments foreseen in the LGPD, as well as to establish a dialogue of sources with other existing procedural diplomas, indicating the potential and difficulties in the protection of data on security.

Keywords: collective protection, data protection, individual protection, LGPD, procedural aspects.

*Mestrando em Direitos Coletivos e Cidadania pela Universidade de Ribeirão Preto (UNAERP).
E-mail: denyeduardo.academico@gmail.com

**Mestre e Doutor em Direito das Relações Sociais pela PUC de São Paulo.
E-mail: adalbertosimao@uol.com.br

*** Doutorado em Economia comportamental pela Pontifícia Universidade Católica de Goiás (PUCGO). Professor efetivo da Pontifícia Universidade Católica de Goiás - (PUCGO), Universidade Salgado de Oliveira (UNIVERSO), Centro Universitário Alves Faria (UNIALFA/FADISP).
E-mail: diogenes_carvalho@ufg.br

INTRODUÇÃO

Com a sanção da Lei Federal nº 13.709, de 14 de agosto de 2018 intensificaram-se as discussões a respeito da importância da disciplina no tratamento de dados pessoais dos sujeitos.

Vazada em 65 artigos e sem motivação de sua edição através de "considerandos", a LGPD, abreviação de Lei Geral de Proteção de Dados, não trouxe apenas a disciplina de aspectos materiais sobre proteção de dados, mas também tratou de disciplinar procedimentos de garantia e efetivação.

Através de uma análise bibliográfica e documental, seguindo-se pelo método dialético na coleta, compilação, comparação e crítica dos dados, o presente trabalho pretende ampliar horizontes a respeito dos instrumentos de concreção dos direitos individuais, coletivos e cidadania, no tocante ao aspecto de disciplina da LGPD.

As discussões científicas sobre a LGPD até o momento voltaram-se para seus aspectos de direito material, havendo um volume significativo de trabalhos nesse contexto. Porém, não se pode desprezar os aspectos de direito processual e procedimental para concretude da norma, sob pena de conferir-lhe o título de natimorta.

Busca-se, assim, descrever e correlacionar os instrumentos de tutela individual e coletiva que poderão ser utilizados no âmbito da LGPD, em âmbito extrajudicial e judicial, possibilitando prever situações e as suas possibilidades de enfrentamento.

1 PANORAMA GERAL DA LGPD E AS INFLUÊNCIAS DO DIREITO COMPARADO

A realidade do mundo globalizado é a conexão e interoperabilidade entre as mais diversas tecnologias. Se no século passado o surgimento dos aparelhos de telefone celular e da conexão de internet discada representaram avanços da sua época, hoje, a absorção dessas tecnologias e sua evolução, apenas nas duas primeiras décadas deste século, são indicativos do surgimento de novos fatos materiais a atuarem na sociedade, exigindo regulamentação legal.

Tratam-se das preocupações inerentes à quinta dimensão dos direitos fundamentais, referida por Zimmermann e Condeixa (2015) como sendo os direitos relacionados à realidade virtual, ao ciberespaço, diante da açodada capacidade de difusão de informações.

A tutela desses novos direitos, dentre os quais o da proteção de dados coletados, gerados, armazenados e tratados por meio eletrônico, induziram o surgimento de áreas ou subáreas do direito fundamentadas na *"*afirmação permanente das necessidades humanas e na legitimidade de ação dos novos sujeitos sociais*"* (WOLKMER, 2002, p. 27).

Trata-se do direito de autodeterminação afirmativa, incorporado como um dos fundamentos da Lei Geral de Proteção de Dados (art. 2º, inciso II), que importa na garantia eficaz de defesa e controle dos seus dados pessoais, um desdobramento da dimensão protetiva da liberdade, privacidade e desenvolvimento da pessoa natural (FRAZÃO; OLIVA; ABILI, 2019).

Assim, o advento do comércio eletrônico, a imersão da vida cotidiana através de aplicativos de celular, culminando com a internet das coisas, demonstraram que as relações jurídicas decorrentes da utilização dos meios de tecnologia da informação resvalavam na hipossuficiente regulamentação normativa interna, já que a normatização do Código Civil e algumas poucas leis esparsas se mostravam, desde logo, obsoletas.Já na década de 90, Beppler (1998, p. 121) sustentava a respeito da necessidade de:

> ...um Direito Civil da Informática e um Direito Penal da Informática. O primeiro englobaria relações privadas e que envolvem a utilização da informática, como, por exemplo, programas, sistemas, direitos autorais, transações comerciais, entre outros. O segundo, o Direito Penal da Informática (...) diz respeito às formas preventivas e repressivas, destinadas ao bom e regular uso da informática no cotidiano.

Com um avanço significativo dessas tecnologias, a situação de vazio normativo se potencializava em virtude da condição transfronteiriça da internet e pela existência de redes paralelas ilícitas, de difícil rastreamento, como a *darkweb*[1].Nesse contexto, Follone e Simão Filho (2020, p. 939) alertam:

> Embora não pareçam, as novas tecnologias da informação podem ser nocivas aos consumidores, pois, a adoção de referidas tecnologias possibilita o tratamento em massa de dados pessoais o que dificulta essa percepção e podem transparecer outras possibilidades de poder. A uma porque a disponibilidade indiscriminada de dados pessoais dos consumidores aos fornecedores resulta em aumento de bens e serviços personalizados. E, a duas, porque pode gerar discriminação ao consumidor no mercado.

Através desta matriz de riscos e possibilidades, o multilateralismo exigiu que o Brasil se adequasse às novas tendências de proteção de dados, não somente por reconhecer a necessidade de proteção à pessoa, mas também em função dos mercados os quais o país possui participação real, como o comércio com a União Europeia.

O simples fato de o país possuir relações comerciais de cunho internacional exigiu que houvesse uma disciplina adequada de tratamento de dados, pois a ausência de proteção a dados coletados nos negócios transnacionais se tornaria um desestímulo ao mercado.

O Regulamento de Proteção de Dados da União Europeia – GDPR-EU 2016/679 traz previsões acerca da transferência de dados pessoais protegidos pela legislação no âmbito do direito internacional, seja para um país terceiro ou um organismo internacional (REGULAMENTO (UE)..., 2016).

Segundo o artigo 45 da GDPR-EU, a transferência de dados somente pode ocorrer se a Comissão da União Europeia tiver certificado que o país terceiro, um território ou um ou mais

1 Segundo GREENBERG (2017, p. 1): trata-se de uma coleção de centenas de sítios eletrônicos que se utiliza de ferramentas de anonimização de protocolo TCP/IP, sendo mais comumente utilizada para o comércio ilícito de drogas e pornografia infantil, sendo também utilizada para a realização de denúncias anônimas e proteção de usuários contra censura e vigilância.

setores específicos desse país, ou a organização internacional, tenham assegurado um nível de proteção adequado.

Os critérios utilizados pela Comissão para a definição da autorização dizem respeito:

(i) ao controle legal exercido, de acordo com o Estado de Direito, com respeito aos direitos humanos e liberdades fundamentais tanto pela legislação genérica, quanto específica, especialmente no tocante à segurança pública, defesa, segurança nacional e direito penal, com especial observância do acesso das autoridades públicas aos dados pessoais e a disciplina de tratamento desses dados para transferência a outros países ou organismos;

(ii) à existência e ao efetivo funcionamento de uma autoridade de controle, independente, responsável por assegurar e impor o cumprimento das regras de proteção de dados, com poderes coercitivos e podendo tratar as demandas dos titulares dos dados no exercício dos deus direitos;

(iii) os compromissos internacionais assumidos pelo país ou pela organização internacional com relação à proteção de dados pessoais, bem como a sua participação em organismos multilaterais ou regionais, especialmente aqueles relacionados à proteção de dados.

Caso não haja a autorização da Comissão para esta transferência de dados as operações de tratamento somente podem ocorrer se houverem garantias adequadas e se os titulares dos direitos possuírem possibilidade de oposição à essa transferência e medidas jurídicas corretivas e eficazes (art. 46, GDPR-EU).

O tratamento pode ocorrer ainda que não haja autorização da Comissão desde que haja (i) um instrumento jurídico vinculante e com força executiva entre autoridades e organismos públicos; (ii) regras vinculantes aplicáveis às empresas; (iii) cláusulas pré-formatadas de proteção de dados, previamente analisadas e aprovadas pelo Comitê de controle de execução dos atos da Comissão da União Europeia; (iv) código de conduta com compromissos vinculantes e força executiva adotados pelo responsável pelo tratamento dos dados na União Europeia e pelo país terceiro ou (v) o procedimento de certificação, mediante selos e marcas de proteção de dados, concedidos pelo Comitê de controle ou a própria Comissão.

Portanto, a rapidez[2] com que surgiu um estatuto de proteção de dados pessoais no Brasil decorreu não somente de necessidade de proteção à pessoa, mas também, com cunho relevante, para possibilitar competitividade e manutenção das relações multilaterais brasileiras.

2 ÂMBITO DE PROTEÇÃO E COMPETÊNCIA RESOLUTIVA: CONSIDERAÇÕES SOBRE DADOS PESSOAIS SENSÍVEIS, ANONIMIZADOS E A RESPONSABILIDADE E LEGITIMIDADE DOS OFICIAIS DE PROTEÇÃO DE DADOS (*DPO'S*)

Não se olvida que o maior bem jurídico a ser protegido pela Lei Geral de Proteção de Dados é a privacidade (BRASIL, 1988, art. 5º, X), não à toa que este é também seu primeiro

2 O Projeto de Lei nº 4.060/2012 do Deputado Milton Monti, apresentado em 13/06/2012 transformou-se na Lei Geral de Proteção de Dados em 14/08/2018, tempo este que se considera relativamente curto para uma proposta legislativa dessa natureza se tornar lei.

fundamento estruturante (BRASIL, 2018a, art. 2º, I).

Trata-se da proteção de todos os aspectos, ou esferas, da vida privada, como se referiu Hubmann e Henkel (1950 apud CUNHA; SIMÃO FILHO, 2017, p. 270), ao conceberem a Teoria dos Círculos Concêntricos, segundo a qual a vida privada possui três círculos, ou esferas, que merecem proteção jurídica estatal. Isto é, a esfera do segredo é abrangida pela esfera da intimidade ou da confidência, que por sua vez estão abrangidas na esfera da privacidade em sentido lato.A LGPD abarca a proteção de todas estas esferas da vida privada.

Aquilo que está na esfera do segredo está com o maior grau de proteção, notadamente em virtude de, no mais das vezes, referirem-se a dados os quais o sujeito revela a um círculo bastante diminuto de pessoas, de sua estrita confiança. É o que ocorre, por exemplo, com alguns dados relacionados à saúde e à vida sexual do sujeito (infecção por doença específica, orientação sexual, submissão a tratamentos experimentais, etc).

Já no que diz respeito à esfera da intimidade ou confidência temos os dados que o sujeito pode querer evitar comentários ou maiores ilações a respeito, como por exemplo, uma opinião política, uma convicção religiosa, ou mesmo sua origem étnica (apoiadores ou opositores a determinada corrente política ou político, convicção a respeito de temas sensíveis à religiosidade, como o aborto, o casamento homoafetivo, dentre outros).

Percebe-se, contudo, que a LGPD foi bastante criteriosa no tratamento desses dados, classificando-os como sensíveis, na forma do artigo 5º, inciso II.

O tratamento conjunto desses dados, tornando-os praticamente pertencentes à mesma esfera, para fins práticos, demonstra um avanço e um ganho de proteção. Em termos doutrinários, ainda se mostra relevante a sua diferenciação, pois tal reverbera no maior ou menor grau de lesão à proteção que se pretende conferir à privacidade.

É que a LGPD ao tratar tais dados em conjunto permite maior liberdade ao sujeito para ele próprio classificar, em seu íntimo, aquilo que pretende incluir em cada esfera de proteção, ora apenas na intimidade ou confidência, ora na maior proteção da esfera do segredo.

Não poderia a lei, por consequência, classificar por ela mesma aquilo que encontra-se nos insondáveis domínios do afeto (BRASIL, 2011, p. 4) e da gama ampla de convicções de qualquer espectro. Cada um há de ter o próprio direito de se comportar conforme ache mais conveniente, de modo que para alguns, revelar o diagnóstico de uma doença sob a qual ainda pairam incertezas e preconceitos significa exposição incomensurável e, para outros, o tratamento e exposição pública deste diagnóstico é uma arma de militância política e social de esclarecimentos, para vencer as barreiras do preconceito.

Porém, por este mesmo exemplo é possível antever que a diferenciação doutrinária trazida pela Teoria dos Círculos Concêntricos também permite valorar a extensão do dano causado em virtude de divulgação indevida de dados sensíveis. Para aquele que trata o diagnóstico médico da doença uma exposição por demais deletéria, o dano será significativamente maior do que aquele cuja divulgação sistemática e incentivada do mesmo diagnóstico não encontra-se contido na esfera do segredo.

Os dados anonimizados são conceituados na LGPD como os "*dado[s] relativo[s] a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento"* (BRASIL, 2018a, art. 5º, III).

Tratam-se dos dados que já são colhidos de forma anônima, sem identificação exata do sujeito a que se refere, ou aqueles dados que após tratamento tornam-se impossíveis de serem atrelados a uma pessoa.

Esses dados são comumente colhidos e utilizados em pesquisas científicas e estatísticas, cujo tratamento de dados só é possível por consentimento livre e esclarecido ou garantia, sempre que possível, da anonimização (BRASIL, 2018a, art. 7º, incisos I e IV).

. Porém, esses dados também são coletados na grande maioria das atividades diárias modernas, como assevera Simão Filho (2015 apud SIMÃO FILHO; SCHWARTZ, 2016, p. 316):

> As informações geradas em ligações telefônicas, call centers, troca de e-mails, endereços de busca na internet, uso de caixas e equipamentos eletrônicos, qualidade de postagens em redes sociais ou interesses demonstrados em compras de qualquer natureza, são assim captadas, armazenadas e processadas para compor ou completar um banco de dados específico.

A esse tipo de banco de dados deu-se o nome de *Big Data*, cuja capacidade de operação está intimamente ligada à captação, tratamento, monetização, replicação e previsão de comportamentos e padrões.

Esses dados anonimizados mantém íntima relação com a operação de tratamento automatizado – que é o núcleo dos *Big Datas* – e cujos instrumentos de tutela específica serão tratados a seguir.

A titularidade dos dados pessoais é da pessoa natural (BRASIL, 2018a, art. 17).
sempre garantidos os direitos fundamentais da liberdade, intimidade e privacidade. Este é o direito básico reconhecido pela norma, apto a evitar questionamentos acerca da propriedade de bancos de dados que agora ganha compreensão distinta: a propriedade é da pessoa a que se referirem os dados contidos no banco, os agentes de tratamento e o encarregado são apenas responsáveis pela sua guarda, utilização e tratamento, nos estritos limites da lei.

Os agentes de tratamento são o operador e o controlador. Operador é aquele que realiza o tratamento dos dados, em nome – leia-se: sob as ordens e regulamentos – do controlador. Este último é a quem compete as decisões sobre o tratamento dos dados pessoais. Ambos podem ser pessoas naturais ou jurídicas, de direito público ou privado.

Por fim, o encarregado é aquele que será indicado pelo controlador (BRASIL, 2018a, art. 41) para aceitar comunicações e reclamações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da Autoridade Nacional e adotar providências, orientar os funcionários e contratados da entidade sobre as práticas para proteção de dados pessoais e, ainda, executar as demais atribuições definidas pelo controlador ou por normas complementares.

Já a Autoridade Nacional de Proteção de Dados (ANPD) é órgão da administração

pública federal, integrante da Presidência da República, que poderá vir a se tornar autarquia de regime especial por transformação (BRASIL, 2018a, art. 55-A e §1º). A Autoridade Nacional possui garantia de autonomia técnica e decisória, dirigida por um Conselho Diretor com 05 (cinco) Diretores, dentre os quais um será seu Diretor-Presidente que, pelo princípio da hierarquia administrativa, será o representante legal, judicial ou extrajudicial, da ANPD.

Estas considerações são necessárias para a compreensão exata dos aspectos processuais da proteção dos dados, tendo em vista as condições da ação, incluindo-se a legitimidade passiva da parte, questões estas a serem abordadas no capítulo seguinte.

3 INSTRUMENTOS PROCESSUAIS ADMINISTRATIVOS

O volume de dados coletados e tratados no mundo é deveras incontável. Considerando-se apenas o Brasil, dados do IBGE de 2018 revelam uma população de aproximadamente 209,5 milhões de pessoas. Se cada uma dessas pessoas utilizar seus dados pessoais como nome, filiação, endereço de residência e trabalho e número de apenas um telefone de contato, teremos cerca de 1,04 bilhão de dados pessoais protegidos a serem geridos num único banco.

Esta situação hipotética é suficiente a se constatar que para que a LGPD possua eficácia, os instrumentos à disposição dos titulares dos dados devem ser os mais amplos possíveis, no âmbito judicial e extrajudicial, mediante procedimentos céleres, inclusive sumários, que impeçam que essas demandas sejam redirecionadas para o caminho da judicialização.

Como se trata de uma legislação ainda em implementação, este é o momento crucial para que se determine a eficácia da LGPD.

Foram previstos alguns instrumentos administrativos para que o titular de direito à proteção de dados pessoais se valha, dando concretude ao direito material.

No âmbito das entidades de direito público o processamento de quaisquer dos pedidos será regido pela norma que discipline o processo administrativo em cada ente, aplicando-se subsidiariamente, ou no caso de ausência de norma sobre o tema, a Lei Federal nº 9.784/99 (BRASIL, 1999), tal como previsto no artigo 23, §3º da LGPD (BRASIL, 2018a). Quanto às entidades reguladas pelo direito privado, a definição dos procedimentos para reclamações e petições de titulares de dados, bem como as obrigações específicas para os diversos envolvidos no tratamento, serão definidas pelo controlador e os operadores através de manuais de boas práticas e de governança (BRASIL, 2018a, art. 50).

No aspecto procedimental, a LGPD define as normas gerais (BRASIL, 1988, art. 24, XI e §§1º e **2º e art. 30, incisos I e II**) em matéria processual. Há margem para legislação suplementar pelos Estados e Municípios, que poderão regulamentar desde os requisitos mínimos do pedido inicial, até mesmo os prazos de tramitação, a forma de obtenção das provas necessárias à comprovação dos fatos, requisitos do ato decisório final, dentre outros aspectos.

Em qualquer hipótese, tanto no âmbito público quanto privado, a Autoridade Nacional

de Proteção de Dados possui competência para expedição de regulamentos e procedimentos sobre dados pessoais e privacidade (BRASIL, 2018a, art. 55-J, XIII da LGPD), que deverão ser observados nas regulamentações internas de cada ente.

3.1 Requisição ao Controlador (art. 18, LGPD)

O titular dos dados tem a sua disposição a requisição de informações e o requerimento para providências, que serão dirigidas ao controlador para cumprimento.

O texto legal utiliza-se de duas terminologias diferentes que, intencionalmente ou não, conduzem a destinos distintos o pedido do titular dos dados.

Requisição é instituto próprio do direito constitucional e administrativo. Ao analisar a possibilidade de requisição de documentos e informações pelo Ministério Público ao Poder Judiciário, em parecer jurídico, Ataliba (1992, p. 337) tece os seguintes comentários sobre o instituto:

> A palavra "requisição", no direito brasileiro, é muito forte! É termo técnico-jurídico do direito constitucional positivo, embora implícito, tradicionalmente aplicado ao uso compulsório da propriedade privada (móveis e imóveis) pela Administração, em casos de guerra ou "perigo público" (calamidades, convulsões, etc.).

As requisições administrativas sempre decorrem da lei em sentido estrito e, sendo atos administrativos, estão dotadas do atributo da autoexecutoriedade, ressalvando-se a apreciação judicial da legalidade do ato (ATALIBA, 1992, p. 337).

Também há a presença da requisição, para obtenção de informações e documentos de interesse à instrução do inquérito civil, prevista no artigo 8º, §1º da Lei nº 7.347/85 (BRASIL, 1985), sendo possível a negativa de seu fornecimento somente quando houver imposição legal de sigilo, suprível por decisão judicial. O desatendimento da requisição ministerial mediante *"a recusa, o retardamento ou a omissão"* é penalmente tipificado, na forma do artigo 10 da Lei nº 7.347/85 (BRASIL, 1985).

Agora, com o advento da LGPD nos parece que a requisição passa a ser instrumento jurídico mais amplo, utilizável pelo titular dos dados, ou seja, a pessoa natural, para exercício direto e autoexecutável, dos direitos previstos nos incisos III, IV, V, e IX do artigo 18 (BRASIL, 2018a).

Estas hipóteses tratam de situações em que incabível, ao menos em tese, o indeferimento de sua execução pelo controlador, tendo em vista dizerem respeito direto à liberdade de permitir ou não a utilização dos dados. É o caso de atuação sumária do controlador, sem maiores delongas ou perquirições ao titular.

Não caberia, por exemplo, que o controlador indeferisse pedido de revogação de consentimento, já que a própria lei confere direito líquido e certo a isto (BRASIL, 2018a, art. 8º,

§5º).

A sumariedade no atendimento da requisição vem expressa na primeira parte do §4º, do artigo 18 da LGPD (BRASIL, 2018a), que admite postergação apenas no caso de impossibilidade fática – quando a requisição for dirigida a quem não seja agente de tratamento dos dados referidos ou diante de qualquer fato impeditivo do atendimento – ou jurídica – quando houver fundamento legal que autorize o controlador a agir de modo diverso daquele esperado pelo titular (BRASIL, 2018a, art. 18, §4º, segunda parte e incisos I e II).

A requisição será exercida de modo gratuito pelo titular, não sendo possível que a lei estabelecesse de outra forma, já que a ação de *habeas data*, típica para a tutela de dados pessoais, encontra previsão constitucional de gratuidade (BRASIL, 1988, art. 5º, LXXVII).

O artigo 19 da LGPD (BRASIL, 2018a) também menciona a requisição, contudo compreendemos que neste ponto há uma má redação legislativa, sendo mesmo caso de requerimento, conforme se verá no tópico a seguir.

3.2 Requerimento ao Controlador (art. 18, §3º, LGPD)

Em sentido diverso da requisição, o requerimento ao controlador enseja análise, poderá necessitar de instrução probatória, e está sujeito a juízo de mérito do controlador, com deferimento ou não do pedido, desde que fundamentado.

Embora a redação do §3º do artigo 18 (BRASIL, 2018a) não especifique quais direitos serão submetidos a requisição e quais outros serão objeto de requerimento, a diferenciação técnico-jurídica trazida no tópico anterior bem revela a importância dessa distinção.

Serão objeto de requerimento, no nosso entendimento, todos os direitos os quais digam respeito à obtenção de informações sobre o tratamento de dados e a hipótese de sua eliminação, após confirmação da inexistência de situação impeditiva. Isto é, será motivo de requerimento os direitos previstos nos incisos I, II, VI, VII e VIII do artigo 18 (BRASIL, 2018a).

Neste caso não há como vislumbrar a sumariedade do pedido pois para se confirmar a existência de tratamento, por exemplo, o controlador terá de instruir o pedido com documentação pertinente a isso atestar (certidões, respostas a consultas, memorandos, ofícios, etc), já que este é o procedimento mais compatível com as boas práticas de comunicação entre titular e agentes de tratamento, conforme o princípio da transparência (BRASIL, 2018a, art. 50, §2º, inciso I, alínea "e"), trata-se de informação que afeta direitos e interesses, exigindo motivação do Poder Público (BRASIL, 1999, art. 50) e atende ao dever de informação do consumidor (BRASIL, 1990a, art. 6º, inciso III).

Também no caso do requerimento haverá o processamento gratuito do pedido, sendo importante destacar que não importa o custo para o controlador para atendimento da demanda que lhe for imposta, todos os atos serão gratuitos, não se admitindo, por exemplo, que o envio de resposta ao requerimento, por carta ao titular, tenha cobrança desse custo, pois o dever de resposta

é ônus legal.

Interpretação diversa, em nossa compreensão, não encontra albergue no Código de Defesa do Consumidor (BRASIL, 1990a, art. 51, XII), viola o princípio da responsabilização e prestação de contas (BRASIL, 2018a, art. 6º, X) e macula a regularidade do *compliance* em tratamento de dados (BRASIL, 2018a, art. 43, II).

3.4 Direito de Petição à ANPD (art. 18, §1º, LGPD)

É certo que o sistema de comunicação entre o controlador e o titular dos dados foi concebido para que possa funcionar com regularidade, tal como o tratamento das demandas dos consumidores diretamente pelos fornecedores.

Em havendo falha ou omissão do controlador, todavia, há remédio administrativo que constitui verdadeiro sistema hierarquizado de proteção de dados, mediante o qual o titular poderá exercer seu direito de petição a Autoridade Nacional de Proteção de Dados – ANPD, materializando direito fundamental do artigo 5º, XXXIV, alínea "a" da Constituição (BRASIL, 1988).

É condição essencial do recebimento e processamento dessa petição a demonstração de que o controlador não solucionou a questão dentro do prazo regulamentar (BRASIL, 2018a, art. 55-J, inciso V).

Ressaltamos, contudo, que essa condição não pode ser interpretada como *sine qua non* para acionamento da ANPD. Nos casos em que sequer haja a identificação do controlador, que é obrigatória (BRASIL, 2018a, art. 9º, incisos III e IV), ou não havendo estrutura implementada para recebimento das requisições e requerimentos, o acionamento da ANPD deve ser feito sem a prévia tentativa de solução junto ao controlador.

A petição deverá ser dirigida ao Presidente do Conselho-Diretor da ANPD. O Conselho determinará, então, o encaminhamento da petição à unidade competente da ANPD para instrução (BRASIL, 2020a, art. 4º, inciso VI, alínea "a" do Anexo I ao Decreto nº 10.474, de 26 de agosto de 2020 – Regulamento da ANPD).

Há possibilidade de delegação da competência do Conselho-Diretor para os órgãos internos da ANPD, conforme autorizado no artigo 31, do Regulamento (BRASIL, 2020a).

Ao apreciar o pedido, a ANPD poderá determinar qualquer providência, comissiva ou omissiva, no atendimento dos interesses do titular, sendo cabível até mesmo a adoção de medidas preventivas, isto é, cautelares, com fixação

O Regulamento criou uma outra classe processual, com natureza recursal, no âmbito interno da ANPD: o pedido de reexame. Trata-se de pedido para que o Conselho-Diretor reavalie a decisão tomada através da competência delegada, pronunciando-se em última instância sobre o caso.

Os Conselheiros da ANPD possuem poder decisório, nos processos de sua relatoria, sendo possível a definição de julgamentos singulares, conforme o artigo 26, incisos I e II do Regulamento

(BRASIL, 2020a). Isso acarreta, por óbvio, a previsão da existência de, no mínimo, um recurso hierárquico para apreciação colegiada, conforme garantia constitucional e legal (BRASIL, 1988, art. 5º, LIV e LV; BRASIL, 2018a, art. 55-J, inciso IV; BRASIL, 2020a, art. 2º, inciso IV).

3.5 Direito de Petição aos Órgãos de Defesa do Consumidor (art. 18, §8º, LGPD)

A massiva maioria dos consumidores não dominam conceitos e conhecimentos que lhes habilite a buscar, ainda que administrativamente, a proteção de seus dados pessoais, invocando dispositivos legais correspondentes.

Mas é princípio da LGPD a transparência e a responsabilização (BRASIL, 2018a, art. 6º, VI e X). Não se pode conceber que haja responsabilização sem que o acesso dos consumidores e titulares dos dados seja facilitado, pois não é de agora que isso é reconhecido como direito básico (BRASIL, 1990a, art. 6º, VIII).

A intimidade entre a LGPD e o direito do consumidor é mais do que evidente, é inegável. Traçando esta relação conceitual Carvalho e Ferreira (2018) atestam:

> A defesa do consumidor e a proteção de dados pessoais visam proteger o cidadão de um desequilíbrio de poderes que possa afetar a tomada de uma decisão livre, autônoma e informada. Enquanto a defesa do consumidor busca reequilibrar a relação entre consumidor e fornecedor no mercado de bens e consumo, a proteção de dados diz respeito ao reequilíbrio entre controlador dos dados pessoais e o titular, que muitas vezes desconhece como se dá o tratamento de dados, suas finalidades ou os seus possíveis riscos.

Aos órgãos de defesa dos consumidores também incumbirá dar tratamento às demandas relacionadas aos direitos tutelados pela privacidade de dados na internet. A capilaridade destes órgãos e a especializada competência no atendimento das demandas consumeristas permitirão conferir eficácia às reclamações por desvios e ilicitudes cometidas com relação aos dados dos titulares.

3.6 Pedido de Revisão de Decisão com Base em Dados Automatizados

O tratamento de dados é a base da internet para que ela consiga ofertar, com relevância, as informações e produtos que o consumidor deseja ou necessita.

A Internet das Coisas (IoT) tem a capacidade de interconectar uma rede de objetos, que passam a manter uma comunicação integrada entre si e outros sistemas, capturando e compartilhando dados para realização de diversas tarefas, simples ou complexas (CONOSCENTI; VETRO; MARTIN, 2016; SETHI; SARANGI, 2017 apud SAKAMOTO, 2020, p. 14).

Através do tratamento de dados de modo automatizado que diversos aplicativos de celular funcionam. As buscas efetuadas na internet geram dados que são captados e replicados para lojas eletrônicas que ofertam produtos e serviços de acordo com a recente pesquisa.

A Uber utiliza a tecnologia *machine learning* (BRAZIL COMMS, 2018) para identificar riscos com base na análise das viagens, em tempo real, e dessa forma as viagens consideradas potencialmente arriscadas, através de geolocalização do ponto de partida e destino do usuário, são negadas, salvo se o usuário fornece mais dados de identificação que, obviamente, passarão por novos tratamentos aptos a definir seu perfil e permitir a tomada de decisão pela fornecedora das viagens.

Contra este tratamento automatizado de dados a LGPD garante o direito de solicitação de revisão dessas decisões robotizadas, que afetam interesses, inclusive os relacionados à definição de perfil *"pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade"* (BRASIL, 2018a, art. 20).

Ao controlador, neste caso, incumbe, além de proceder com a própria revisão do tratamento automatizado, fornecer informações sobre como estes dados são tratados, com quais critérios e mediante quais procedimentos. A ressalva das informações encontra guarida no sigilo industrial e comercial.

É garantido, contudo, através de petição à ANPD (vide tópico 3.3) que esta realize auditoria junto ao controlador para analisar os critérios adotados, se discriminatórios ou não.

4 INSTRUMENTOS PROCESSUAIS DE TUTELA JURISDICIONAL INDIVIDUAL E COLETIVA

A tutela dos direitos relacionados à privacidade dos dados não está excluída da função jurisdicional, em decorrência da inafastabilidade da jurisdição, bem como por que reconhecida a tutela individual e coletiva (BRASIL, 2018a, art. 22).

Não se nega acerca da inexistência de monopólio jurisdicional na questão haja vista a possibilidade de utilização da arbitragem para solução dos casos individuais, tanto no setor público (arbitragem exclusivamente de direito, conforme o artigo 1º, §1º e artigo 2º, §3º da Lei de Arbitragem) (BRASIL, 1996), quanto no setor privado (arbitragem de direito ou de equidade, conforme art. 2º, *caput* da mesma Lei) (BRASIL, 1996).

4.1 Instrumentos exclusivos de tutela individual

Nesta seção trataremos a respeito dos instrumentos judiciais que não admitem substituição processual, sendo exercidos pelos próprios titulares dos direitos em hipótese de legitimação ordinária.

4.1.1 Habeas data (Lei nº 9.507/97)

O *habeas data* **é um remédio constitucional (**BRASIL, 1988, art. 5º, LXXII) que tem por objetivo proteger a privacidade da pessoa natural contra usos abusivos de dados pessoais, coletados por meios fraudulentos, desleais ou ilícitos; tratamento realizado com relação a dados sensíveis ou a conservação de dados falsos ou com fins diversos daqueles que a lei autoriza (SILVA, 2007, p. 453).

Trata-se de ação isenta do pagamento de custas (BRASIL, 1997, art. 21), proposta em face de pessoas jurídicas de direito público interno, ou pessoas jurídicas de direito privado que atuem em colaboração ou delegação de serviços públicos

> que prestem serviço para o público ou de interesse público, envolvendo-se aí não só concessionários, permissionários ou exercentes de atividades autorizadas, mas também (...) instituições de cadastramento de dados pessoais para controle ou proteção do crédito ou divulgadoras profissionais de dados pessoais. (SILVA, 2007, p. 455).

No caso da defesa dos direitos previstos na LGPD, a utilização do *habeas data* somente pode ser feita por pessoa natural, já que são protegidos apenas os dados pessoais.

Descabe o *habeas data* preventivo, sendo imprescindível a comprovação de acionamento prévio do controlador, apontando-se na petição inicial, cuja representação técnica por advogado é obrigatória, quais as providências adotadas que não satisfazem a pretensão do titular ou a omissão na tomada de providências (BARROSO, 1998, p. 156-157; BRASIL, 1990b, p. 2).

O direito de ação é, em regra, personalíssimo (SILVA, 2007, p. 454) e individual. Entretanto, a coletivização do processo mostra uma tendência de que seja admitida a impetração do *habeas data* também como ação coletiva, em virtude de esta ser o único meio efetivo de acesso à Justiça pelos grupos sociais, em especial dos grupos mais vulneráveis, do ponto de vista econômico e social (BRASIL, 2018b, p. 15).

Mourão Neto (2021) defende a possibilidade do manejo do *habeas data* coletivo em virtude da dimensão que podem assumir a violação dos direitos de proteção de dados nas relações de consumo, cuja massificação lhe é inerente, como também por nós comentado no tópico 3 deste trabalho.

Assim, o *habeas data* poderá ser utilizado, no âmbito da LGPD, quando não houver tratamento adequado dos dados, ainda que haja consentimento, para proteção dos direitos previstos nos artigos 18 e 20, para determinação de exclusão de dados e para exigência de providências em face dos agentes de tratamento.

5.1.1 Ações cíveis em geral

Pela obviedade não nos deteremos com maiores minúcias quanto ao fato de que é garantido ao titular dos direitos a propositura de ações cíveis em geral, declaratórias, constitutivas e condenatórias em face dos agentes de tratamento e da pessoa, física ou jurídica, que se utilizar

dos dados pessoais à margem do que estabelece a LGPD.

Ressalta-se porém que a LGPD permite, agora, um novo panorama na causa de pedir e nos pedidos dessas ações cíveis, em virtude da positivação de direitos que anteriormente ficavam a cargo apenas do reconhecimento judicial, mediante processo hermenêutico de pouca segurança jurídica.

Conforme salientamos anteriormente (tópico 3) a LGPD traz a classificação dos dados pessoais em dados sensíveis, o que constitui-se como bússola ao magistrado na definição da extensão do dano provocado em virtude do tratamento indevido desses dados do titular, podendo valorar melhor a indenização a ser deferida. Quanto mais sensíveis os dados utilizados na ação ilícita ou abusiva, maior será a extensão do dano, a exigir maior reparação (art. 186, 187 e 944, do Código Civil).

Tratando-se de responsabilidade civil aquiliana, admite-se a análise da culpa da vítima, exclusiva ou concorrente, quanto ao seu comportamento com relação ao tratamento dos seus dados (omissão na adoção de providências de segurança recomendadas pelo controlador, por exemplo, tal como a instalação de sistemas de segurança, desconsideração de alertas, etc).

Também com relevo, a prova do vício do consentimento pelo titular incumbe exclusivamente ao controlador, que deverá demonstrar que o obteve em conformidade com a LGPD, sendo vedado o tratamento dos dados obtidos por vício de consentimento (BRASIL, 2018a, art. 8º, §§3º e 4º).

5.2 Instrumentos Exclusivos de Tutela Coletiva

O microssistema de tutela coletiva é constituído, basicamente, pela ação civil pública, ação popular, o mandado de segurança coletivo e o mandado de injunção coletivo. Informa, todavia, o princípio da não-taxatividade ou atipicidade da tutela coletiva que são admitidas todas as espécies de ações capazes de efetivar esta tutela (art. 83, do Código de Defesa do Consumidor).

Neste tópico trataremos especificamente das ações de tutela exclusivamente coletiva, isto é, que somente são admitidas mediante legitimação extraordinária, através de representação processual da coletividade pelos sujeitos legalmente admitidos.

5.2.1 Ação Civil Pública

A ação civil pública é um *"conjunto de mecanismos destinados a instrumentar demandas preventivas, reparatórias e cautelares de quaisquer direitos e interesses difusos e coletivos"* (ZAVASCKI, 2014, p. 53), regulada pela Lei nº 7.347/1985 (BRASIL, 1985) e destinada à proteção contra lesão e a reparação da lesão ao meio ambiente, ao consumidor, à ordem urbanística, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico, bem ainda, à ordem econômica e à economia popular, e a outros direitos ou interesses difusos e coletivos (art. 1º).

Admite-se, ainda, o manejo da ação civil pública na defesa dos direitos individuais homogêneos pelos co-legitimados previstos no artigo 82 do Código de Defesa do Consumidor. Utilizando-se desta legitimação, o Ministério Público do Distrito Federal e Territórios ingressou com a primeira ação civil pública relacionada à LGPD, visando a impedir que uma empresa continuasse a comercializar um banco de dados com informações de cerca de 500 mil pessoas da cidade de São Paulo, cujo consentimento para tanto não havia sido coletado (BRASIL, 2020a).

A ação foi rejeitada, contudo, por falta do interesse de agir já que o portal da empresa, que comercializava o banco de dados, foi tirado do ar por presunção de que iriam *"adequar os seus serviços às normas jurídicas de proteção de dados pessoais"* (VITAL, 2020).

No âmbito das atividades do Poder Público, também sujeito às normas da LGPD, é possível que a ação civil pública seja utilizada para imposição de penalidades pela prática de ato de improbidade administrativa previsto na Lei nº 8.429/92, quando o tratamento de dados não estiver adequado à lei (art. 11, incisos I e II); quando houver o vazamento de dados pelos agentes de tratamento, notadamente quanto a dados sensíveis (art. 11, III), sendo também apenável o recebimento de valores ou bens em função disso (art. 9º), ou ainda, quando não fiscalizada a organização da sociedade civil quanto aos dados de interesse público que são produzidos no decorrer da parceria (art. 10, XIX e Lei nº 13.019/2014), dentre outros atos.

A já discutida massificação das relações consumeristas também permite destacar que eventuais danos sociais, entendidos como aquela espécie de dano coletivo, que tem como consequência a diminuição da qualidade de vida da sociedade ou de determinado grupo social (FRIEDE; ARAGÃO, 2016, p. 22), serão objeto de tutela reparatória coletiva através da ação civil pública, como se vislumbra no caso de utilização de dados relativos a orientação política e filosófica pelo Estado, com critérios discriminatórios negativos, como objeto de censura e coação, apurados mediante controle objetivo na ADPF nº 722 (BRASIL, 2020b).

5.2.2 Ação Popular

A ação popular é resguardada ao cidadão no gozo de seus direitos políticos, podendo ser manejada para anular ato lesivo ao patrimônio público ou de entidade de que o Estado participe, à moralidade administrativa, ao meio ambiente e ao patrimônio histórico e cultural (art. 5º, LXXIII da Constituição).

Tem regulamentação infraconstitucional na Lei nº 4.717/1965, que traz como conceitos para proclamação da nulidade do ato, o vício de competência e de forma, a ilegalidade do objeto, a inexistência dos motivos e o desvio de finalidade (art. 2º).

A compreensão de que a ação popular não protege apenas o patrimônio público material encontra guarida em grandes doutrinadores, como Meirelles, Mendese Wald (2016, p. 195) que afirmam:

> (...) Entender-se, restritamente, que a ação popular só protege o patrimônio

> público material é relegar os valores espirituais a plano secundário e admitir que a nossa Constituição os desconhece ou julga indignos da tutela jurídica, quando, na realidade, ela própria os coloca sob sua égide (CF, arts. 23, VI, 24, VI, 170, VI, e 225). Essa proteção constitucional não deve ser apenas nominal, mas real, traduzindo-se em meios concretos de defesa, tais como a ação popular para a invalidação de atos lesivos desses valores. Se ao Estado incumbe proteger o patrimônio público, constituído tanto de bens corpóreos como de valores espirituais, de irrecusável lógica é que o cidadão possa compeli-lo, pelos meios processuais, a não lesar esses valores por atos ilegais da Administração.

O tratamento de dados pelo Poder Público encontra limitações próprias pois só pode ser efetuado quando necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, III, da LGPD), condicionada sempre aoatendimento 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 (BRASIL, 2018a, art. 20).

Quando o órgão da Administração Pública, portanto, estatui procedimentos viciados de coleta de consentimento de tratamento de dados, está a praticar ato que tende a promover a lesão do patrimônio público, seja pela imposição de penalidades pela ANPD, seja pela reparação de eventuais danos que os agentes públicos causarem, nesta condição, aos particulares (BRASIL, 1988, art. 37, §6º; BRASIL, 2018a, art. 42).

Noutro giro, o servidor que atuante na condição de operador, com capacidade de consulta a dados relativos à propriedade de veículos, por exemplo, que presta essa informação a terceiros, sem consentimento do titular, fora da finalidade pública para a qual instituído o banco de dados, além de praticar eventual falta funcional, poderá sofrer as consequências de uma ação popular, considerando que a jurisprudência tem admitido a aplicação de sanção por ato de improbidade também por meio desse instrumento processual.

Em razão do princípio da integração das ações coletivas, há a concepção de um microssistema processual que contém a lei da ação popular, da ação civil pública e as disposições de tutela coletiva advindas do Código de Defesa do Consumidor, "*com o objetivo de propiciar uma adequada e efetiva tutela dos bens jurídicos nelas previstos"* (BRASIL, 2020c).

6 CONCLUSÕES

A globalização e as exigências do multilateralismo fizeram com que o Brasil editasse a Lei Geral de Proteção de Dados, com vistas à proteção dos consumidores, pessoas naturais, frente a escalada de violações ao direito à privacidade e intimidade, decorrente das novas tecnologias, da massificação das relações consumeristas e da robotização e automatização de procedimentos.

A inspiração na *General Data Protection* da União Europeia (GDPR-EU) permitiu que o Estado brasileiro trouxesse legislação já abalizada, experimentada, funcional e eficaz, utilizada

em toda a Europa ocidental, criando ambiente seguro de investimentos e manutenção das relações comerciais e industriais.

A previsão ampla, própria dos textos constitucionais, da proteção à intimidade, vida privada, honra e a imagem das pessoas (art. 5º, X da Constituição Federal) não se mostrava capaz de socorrer as demandas sociais que surgiam com o avanço da Internet das Coisas e dos *BigDatas*.

Além de prever princípios de relevância para a elaboração dos instrumentos regulatórios pelos atingidos pela LGPD, o texto normativo disciplinou à exaustão a proteção dos dados, trazendo diferenças terminológicas que reverberarão na aplicação do novo marco legal.

Embora não explícita, a desjudicialização na proteção de dados é um princípio implícito da LGPD, diante da criação de um verdadeiro sistema administrativo de resolução de conflitos relacionados à matéria, o que sequer foi previsto, com tamanha minuciosidade, pelo Código de Defesa do Consumidor, ainda que este também tenha trazido inovações para o estado da arte daquela década.

Defendemos que no âmbito administrativo, ao dar aplicabilidade para os dispositivos do marco legal, o intérprete se atente à diferenciação entre os instrumentos de requisição e de requerimento que, aparentemente, foram utilizados como sinônimos, mas que no campo doutrinário ganham diferenciação prática importante.

A positivação na LGPD do conceito de dados sensíveis merece destaque já que pode constituir-se como vetor interpretativo da extensão do dano e da lesão ou ameaça de lesão causada pela indevida divulgação de dados assim qualificados. A adoção da Teoria dos Círculos Concêntricos contribui para esse exercício hermenêutico, mas não esgota, todavia, o seu objeto, que continuará a demandar prova fática da classificação – personalíssima – que cada titular fazia do respectivo dado sensível.

A LGPD traz a presunção da sensibilidade desses dados, mas o sujeito, por deter autodeterminação afirmativa poderá trata-los como um dado pessoal qualquer, disponível para consulta de quem quer que seja em suas redes sociais. A LGPD não transmutou a característica desses direitos, ainda se trata de direitos disponíveis, porém, agora, com amplitude de proteção.

A tutela dos direitos insculpidos na LGPD se confere tanto no campo individual quanto coletivo, pois embora trate-se de direito individual homogêneo, a depender da situação do conflito, este ganhará inegáveis contornos de direitos transindividuais, como no caso da exigência de reparação por danos sociais causados por ato ilícito decorrente do mau uso ou desvirtuamento do tratamento de dados.

Nesse aspecto merece destaque que a ação de *habeas data* tem potencialidade para sair do limbo jurídico do esquecimento, deixando de ser objeto apenas de considerações enciclopédicas e dogmáticas, para passar, de vez, ao campo empírico, da experiência prática, permitindo desenvolver e cultivar a doutrina nacional sobre a ordem de injunção.

A totalidade dos direitos do artigo 18 da LGPD é exercível, no campo jurisdicional, através do mandado de injunção, salvo nos casos de coletivização da demanda, ocasião em que será cabível, via de regra, o mandado de segurança.

O conceito de banco de dados público trazido pela redação da Constituição permite a ampliação desse remédio constitucional inclusive em face de pessoas jurídicas de direito privado, que administrem bancos de dados relacionados a proteção do crédito, por exemplo.

É forçoso reconhecer, todavia, que a Lei nº 9.507/97 não está adequada à modernidade, sendo inolvidável a sua atualização para prever, por exemplo, a possibilidade do seu manejo sem a assistência técnica de advogado, que embora seja essencial à justiça, também não poderá ser diminuído à função de mero despachante de simples pedidos de exclusão ou retificação de dados, negados na seara administrativa por despreparo ou mesmo por intencionalidade do agente de tratamento.

O próprio conceito constitucional de banco de dados público merecia uma interpretação autêntica da norma infraconstitucional para que não pairassem dúvidas sobre a possibilidade de seu manejo contra pessoas jurídicas de direito privado, dada a potencialidade da ordem de injunção, sumária e preferencial sobre um processo de conhecimento.

Reconhece-se, por fim, que a LGPD não inaugura, no campo jurisdicional, novos instrumentos jurídicos, mas se utilizará do sistema de tutela individual e coletiva, com a amplitude possível, para a defesa dos direitos dos titulares de dados.

REFERÊNCIAS

ATALIBA, Geraldo. Poder Judiciário - Ministério Público - Requisição de dados. **Revista de Direito Administrativo**, Rio de Janeiro, v. 187, n. 1, p. 331-342, jan./mar. 1992. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/45099. Acesso em: 05 fev. 2021.

BARROSO, Luis Roberto. A viagem redonda: habeas data, direitos constitucionais e as provas ilícitas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 213, n. 3, p. 149-163, jul/set. 1998. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/47206. Acesso em: 05 fev. 2021.

BEPPLER, Daniela. Internet e informatização: implicações no universo jurídico. In: ROVER, Aires José (org.). **Direito, sociedade e informática**: limites e perspectivas da vida digital. Florianópolis: Boiteux, 2000.

BRASIL. Lei nº 7.347, de 24 de julho de 1985. Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico e dá outras providências. . Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em: 05 fev. 2021.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990a. Dispõe sobre a proteção do consumidor e dá outras providências. . Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 05 fev. 2021.

BRASIL. Lei nº 9.307, de 23 de setembro de 1996. Dispõe sobre a arbitragem. Brasília, DF,

Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9307.htm. Acesso em: 05 fev. 2021.

BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. . Brasília , DF, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 05 fev. 2021.

BRASIL. Lei nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. . Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Acesso em: 05 fev. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 15 ago. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 fev. 2021.

BRASIL. Decreto nº 10.474, de 26 de agosto de 2020a. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. . Brasília, DF, Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Acesso em: 04 fev. 2021.

BRASIL. Ministério Público do Distrito Federal e Territórios. MPDFT ajuíza 1ª ação civil pública com base na LGPD. **MPDFT**, Brasília, 22 set. 2020b. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12384-mpdft-ajuiza-1-acao-civil-publica-com-base-na-lgpd. Acesso em: 05 fev. 2021.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 2**, **de 18 de maio de 1990**. Não cabe o habeas data (cf, art. 5., lxxii, letra "a") se não houve recusa de informações por parte da autoridade administrativa. Brasília: Superior Tribunal de Justiça, 1990b. Disponível em: https://www.stj.jus.br/docs_internet/SumulasSTJ.pdf. Acesso em: 05 fev. 2021.

BRASIL. Supremo Tribunal Federal. Voto. Relator: Ministro Ayres Britto. Disponível em: https://www.conjur.com.br/dl/voto-ministro-ayres-britto-julgamento.pdf. 2011. Acesso em: 04 fev. 2021.

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 143.641/SP. Brasília, DF, 20 de fevereiro de 2018. **Revista Conjur**. Brasília, 20 fev. 2018b. p. 1-56. Disponível em: https://www.conjur.com.br/dl/voto-ministro-ricardo-lewandowski1.pdf. Acesso em: 05 fev. 2021.

BRASIL. Supremo Tribunal Federal. Arguição de descumprimento de preceito fundamental nº 722. Relator: Ministra Cármen Lúcia. Brasília, DF, 22 de outubro de 2020. **Diário da Justiça Eletrônico**. Brasília, 22 out. 2020c. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354. Acesso em: 05 fev. 2021.

BRASIL. Superior Tribunal de Justiça. Agravo Interno no Recurso Especial nº 1875150. Relator: Ministra Regina Helena Costa. Brasília, DF, 11 de novembro de 2020. **Diário da Justiça Eletrônico**, Brasília, 13 nov. 2020d. Disponível em: https://processo.stj.jus.br/processo/eroUnico&termo=08156106620184050000&totalRegistrosPorPagina=40&aplicacao=processos.ea. Acesso em: 05 fev. 2021.

BRAZIL COMMS. Uber adota tecnologia de machinelearning para reforçar prevenção de riscos no Brasil. **UberNewsroom**, São Paulo, 10 abr. 2018. Disponível em: https://www.uber.com/pt-BR/newsroom/uber-adota-machine-learning-para-reforcar-prevencao-de-riscos-no-brasil/. Acesso em: 05 fev. 2021.

CARVALHO, Diógenes Faria de; FERREIRA, Vitor Hugo do Amaral. **Defesa do consumidor ganha com a nova lei de proteção de dados pessoais**. 15 de agosto de2018. Disponível em: https://www.conjur.com.br/2018-ago-15/garantias-consumo-defesa-consumidor-ganha-lei-protecao-dados. Acesso em: 05 fev. 2021.

CUNHA, Tiago Barros; SIMÃO FILHO, Adalberto. A teoria dos círculos concêntricos e a preservação da privacidade humana no registro civil das pessoas naturais.CONGRESSO BRASILEIRO DE PROCESSO COLETIVO E CIDADANIA, 5, 2017, Ribeirão Preto. **Anais** [...]. Ribeirão Preto: Universidade Estadual de Ribeirão Preto, 2017.p. 265-282. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/971. Acesso em: 04 fev. 2021.

FOLLONE, Renata Aparecida; SIMÃO FILHO, Adalberto. A conexão da lgpd e cdc: a proteção de dados pessoais nas relações consumeristas e a sua concretização como direito fundamental. *In*:CONGRESSO BRASILEIRO DE PROCESSO COLETIVO E CIDADANIA, 8, 2020, Ribeirão Preto. **Anais** […].Ribeirão Preto: Universidade de Ribeirão Preto, 2020. p. 937-959.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILI, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. Cap. 10. p. 677-715.

GREENBERG, Andy. **Hacker Lexicon**: whatisthedarkweb? 2017. Disponível em: http://dpya.org/en/images/9/9a/Hacker_Lexicon-_What_Is_the_Dark_Web%3F.pdf. Acesso em: 30 jan. 2021.

MEIRELLES, Hely Lopes; MENDES, Gilmar Ferreira. WALD, Arnoldo. **Mandado de segurança e ações constitucionais**. 37. ed. São Paulo: Malheiros, 2016.

MOURÃO NETO, Samuel Francisco. **Arquivos de consumo (cadastros e bancos de dados de consumidores) e habeas data (individual e coletivo)**. Disponível em: https://www5.pucsp.br/tutelacoletiva/download/artigo_samuel.pdf. Acesso em: 05 fev. 2021.

REGULAMENTO (UE) nº 679, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados. Bruxelas, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN#tocId55. Acesso em: 30 jan. 2021.

SAKAMOTO, Sarah Gomes. **Segurança, privacidade e blockchain no contexto de internet das coisas**. 2020. 66 f. Monografia (Especialização em Internet das Coisas) - Universidade Tecnológica Federal do Paraná, Departamento Acadêmico de Eletrônica, Curitiba, 2020. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/19677. Acesso em: 05 fev. 2021.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 28. ed. São Paulo: Malheiros,

2007. 928 p.

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. Big Data Big Problema!: paradoxo entre o direito à privacidade e o crescimento sustentável. In: CONPEDI LAW REVIEW, 3., 2016, Oñati, Espanha. **Anais [...]**.[S.L.]: Conpedi, 2016. v. 2, p. 311-331. Disponível em: https://indexlaw.org/index.php/conpedireview/article/view/3644/0. Acesso em: 04 fev. 2021.

VITAL, Danilo (ed.). **Primeira ACP baseada na LGPD é indeferida porque site da ré está em manutenção**. 2020. Disponível em: https://www.conjur.com.br/2020-set-23/peticao-inicial-acao-civil-publica-baseada-lgpd-indeferida. Acesso em: 05 fev. 2021.

WOLKMER, Antonio Carlos. Direitos humanos: novas dimensões e novas fundamentações. **Direito em Debate**, Ijui, v. 10, n. 11, n. 16-17, jan./jun. 2002. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/768. Acesso em 28 Jan. 2021.

ZAVASCKI, Teori Albino. **Processo coletivo**: tutela de direitos coletivos e tutela coletiva de direitos. 6. ed. São Paulo: Revista dos Tribunais, 2014.

ZIMMERMANN, Augusto; CONDEIXA, Fábio de Macedo Soares. **Direito constitucional brasileiro**. Rio de Janeiro: Lumen Juris, 2015. t. I.

Como citar: ALVES, Deny Eduardo Pereira; FILHO, Adalberto Simão. CARVALHO, Diógenes Faria de. Instrumentos Processuais de Proteção de Dados. **Scientia Iuris**, Londrina, v. 26, n. 1, p. 105-125, mar. 2022. DOI: 10.5433/21788189.2022v26n1p105. ISSN: 2178-8189.

Recebido em 06/14/2021
Aprovado em 10/20/2021