**DOI: https://doi.org/10.23925/ddem.v.2.n.5.56636**


# MINIMIZAÇÃO E PROPORCIONALIDADE NA COLETA DE DADOS

MINIMIZATION AND PROPORTIONALITY IN DATA COLLECTION

Luiz Carlos Buchain[1]

**RESUMO**
O artigo trata da aplicação do princípio da proporcionalidade na LGPD, analisando-se seu uso em diversos institutos jurídicos criados pela lei, em especial sua incidência sobre os princípios da minimização dos dados e sua conservação no tempo, passando pela regra da exigência de adequação e necessidade dos dados pelo controlador. Os dados só poderão ser utilizados, como regra geral, durante o período não excedente aquele necessário para atender sua finalidade. Embora a lei não fixe em seu texto o conceito de duração do uso dos dados, ela deverá ser entabulada pelo princípio da proporcionalidade, a partir de um critério intrínseco definidor das necessidades atribuídas ao tratamento, mas também tendo em conta os critérios extrínsecos resultantes das normas legais. Já o tratamento de dados sensíveis é, naturalmente, regrado pela proporcionalidade, pois são suscetíveis de criar riscos graves para seus titulares. Por fim, a proporcionalidade também se faz presente quando a lei exige a "análise de impacto" de certos tratamentos de dados, seja em face das relevantes implicações sociais que eles representam, seja pelo emprego de tratamento automatizado o qual, por si só, traz o perigo de criação de "perfis" falsos e tendenciosos do titular. O método de pesquisa utilizado foi o qualitativo tendo a pesquisa bibliográfica e jurisprudencial como metodologia específica.

**Palavras-chave:** dados; proporcionalidade; proteção; análise de impacto.

**ABSTRACT**
The article deals with the application of the principle of proportionality in the LGPD, analyzing its use in several legal institutes created by the LGPD, its impact on data minimization, its conservation over time, passing through the requirement of adequacy and need for data handled by the controller. The data may only be used, as a rule, during the period not exceeding that necessary to meet its purpose. Although the law does not establish the concept of duration in its text, it should be based on the principle of proportionality, based on an intrinsic criterion defining the needs attributed to the treatment, but also considering the extrinsic criteria resulting from legal norms. The processing of sensitive data is, of course, also governed by proportionality, as they are liable to create serious risks for its owners. Finally, proportionality is also present when the law requires the "impact analysis" of certain data processing, either in

[1] Possui graduação em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul (1986), mestrado em DIREITO CIVIL pela Universidade Federal do Rio Grande do Sul (1996) e doutorado em DIREITO ECONÔMICO pela Universidade Federal do Rio Grande do Sul (2005). Atualmente é professor adjunto II da Universidade Federal do Rio Grande do Sul e advogado - BUCHAIN SOCIEDADE INDIVIDUAL DE ADVOCACIA. atuando principalmente nas áreas de direito civil e empresarial, direito administrativo e direito econômico. buchain@buchain.com.br. https://orcid.org/0000-0003-4187-3003.

the face of the relevant social implications they represent, or using automated processing which, in itself, brings the danger of creating false and biased "profiles" of the holder. The research method used was qualitative, with bibliographic and jurisprudence research as a specific methodology.

**Keywords:** data; proportionality; protection; impact analysis.

## INTRODUÇÃO

No século XXI é crescente a atividade de coleta de dados por empresas que ocupam posição de dominação no cenário econômico, o que se refere, muitas vezes, como economia digital. Os dados passaram a representar uma nova fonte de riqueza para tais companhias, o que muito concordam em comparar ao que o petróleo outrora fora. Atualmente há reconhecidos gigantes da economia que assim se tornaram devido a sua habilidade em coletar e processar dados em larga escala: *Facebook*, *Alibaba*, *Amazon* e *Goggle* são exemplos que já se tornaram clássicos dessa nova classe de empresas que têm como característica cobrarem de seus usuários o direito ao uso de seus dados pessoais, e não valores pecuniários (a chamada monetização dos dados).

A Lei Geral de Proteção de Dados nasceu da necessidade social de se estabelecer regras para lidar com esses novos desafios derivados da coleta de dados (FREDES; BORGES, 2021, p. 186), pois os tradicionais instrumentos jurídicos se revelaram obsoletos para o tratamento jurídico dessas questões. Assim há uma nova teoria jurídica para sustentar o direito a privacidade, liberdade e dignidade dos cidadãos (RODOTÁ, 2008, p. 17) frente ao uso do *big data*[2] [3], a qual deverá corresponder a uma respectiva prática jurídica.

[2] *Big Data* (megadados o grandes dados em português) é a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados grandes demais para serem analisados por sistemas tradicionais. Ao longo das últimas décadas, a quantidade de dados gerados tem crescido de forma exponencial. O surgimento da *Internet* aumentou de forma abrupta a quantidade de dados produzidos, e a popularização da Internet das coisas fez sairmos da era do terabyte para o petabyte. Em 2015, entramos na era do zetabytes, e atualmente geramos mais de 2,5 quintilhões de bytes diariamente. O termo *Big Data* surgiu em 1997 e seu uso foi utilizado para nomear essa quantidade cada vez mais crescente e não estruturada de dados sendo gerados a cada segundo. Atualmente o *big data* é essencial nas relações econômicas e sociais e representou uma evolução nos sistemas de negócio e na ciência. As ferramentas de *big data* são de grande importância na definição de estratégias de marketing, aumentar a produtividade, reduzir custos e tomar decisões mais inteligentes. A essência do conceito está em gerar valor para negócios[8]. No que tange a ciência, o surgimento do *big data* representou a criação de um novo paradigma (4° paradigma) sendo concebido um novo método de avançar as fronteiras do conhecimento, por meio de novas tecnologias para coletar, manipular, analisar e exibir dados, construindo valor agregado com as análises geradas. https://pt.wikipedia.org/wiki/Big_data acesso em 20.05.2020.

[3] De acordo com o *Cambridge Dictionary*, o termo *big data* pode ser traduzido para o português como *megadados*, assim definido como uma grande quantidade de dados, produzidos pelos usuários da internet, que somente podem ser guardados e processados a partir de ferramentas e métodos específicos.

A privacidade, tal qual concebida pela LGPD, revela em sua estrutura o chamado direito a "autodeterminação informativa", o qual representa a faculdade de o particular controlar a obtenção, a titularidade, o tratamento e a transmissão de dados a si relativos (TEPEDINO, 2004, p.291). Assim, além de plasmar o direito do cidadão de controlar o conteúdo das informações que lhe digam respeito, a lei exige que se observem certos limites quanto a origem das informações, o momento de sua coleta, seu conteúdo, seu destino e os fins para os quais serão utilizadas, restringindo seu tratamento como ativo comercial das empresas. (BASTOS; ESTEVES, 2021, p. 234). Destarte, embora a limitação da coleta de informações aquelas estritamente necessárias (princípio da necessidade) já estivesse previsto no inciso I, § 3º, art. 3º da Lei 12.414/2011 (que disciplina a consulta a banco de dados para formação de histórico de crédito), a LGPD ratifica a imposição ao controlador da observância do princípio da necessidade[4] para legitimar o tratamento de dados, limitando-os não apenas ao "mínimo necessário", mas também a sua pertinência e *proporcionalidade* em relação a sua finalidade.

Como se vê, como corolário do princípio da necessidade, a lei plasmou o subprincípio da proporcionalidade como elemento que dará a medida dos dados licitamente compilados pelo controlador e destinados a uma determinada finalidade. Como subprincípio informador da necessidade dos dados compilados pelo controlador, a proporcionalidade se revela numa série de regras gerais (aplicáveis a todo tipo de tratamento), e também em regras especiais (aplicáveis somente a certos tratamentos), as quais merecem análise específica. Temos, portanto, um cenário onde a necessidade do uso de dados se intersecta com sua proporcionalidade, exigindo do intérprete e aplicador da lei a observância deste subprincípio como critério de limitação e justificação da necessidade do controlador à coleta de dados.

Para tanto, o artigo está organizado, além desta breve introdução, em duas partes e sua conclusão. A primeira parte trata das regras gerais relativas ao uso mínimo e proporcional dos dados; e a segunda parte trata da aplicação de regras especiais a tratamentos específicos tais como aquele de dados sensíveis ou que representem "riscos graves" ao titular.

O método de pesquisa utilizado na presente pesquisa foi o qualitativo, sendo a pesquisa bibliográfica e jurisprudencial sua metodologia específica.

[4] Art. 6º, III da LGPD.

## 1 – PRINCÍPIOS APLICÁVEIS A TODOS OS TRATAMENTOS

O princípio da minimização e o subprincípio da proporcionalidade irradiam eficácia dentro do sistema legal a todos os tipos de tratamento. São, portanto, princípio e subprincípio de natureza geral revelados tanto na exigência de mitigação dos dados coletados quanto a restrição de sua conservação no tempo.

### 1.1. Minimização, proporcionalidade e finalidade

Todo e qualquer atividade de tratamento de dados deverá se dar sobre dados "adequados" e "necessários" (art. 6º, II e III), sendo os primeiros definidos como a compatibilidade do tratamento com as finalidades informadas pelo controlador ao titular e o segundo como a limitação do tratamento ao mínimo necessário à finalidade para os quais estão sendo tratados. (MIRAGEM, 2019, p. 09-10)

As exigências legais de adequação e necessidade exigem do controlador limitar as características de seu tratamento única e exclusivamente ao que for minimamente indispensável para atingir as suas finalidades. A escolha dos dados tratados é justificada pela finalidade do tratamento ou, seja, deverá haver uma adequação entre a finalidade perseguida e os dados tratados. Assim, se o alcance da finalidade não exige o tratamento de certos dados, os quais foram inclusos no tratamento, esse tratamento poderá ser declarado como desconforme ao subprincípio da proporcionalidade.

Em decorrência do princípio da minimização dos dados (e do subprincípio da proporcionalidade) ancorados no art. 6º, III da LGPD, os dados pessoais devem ser pertinentes e limitados ao que seja necessário para atingir às finalidades para os quais são tratados. O controlador deverá limitar a coleta de dados pessoais ao que seja necessário para alcançar seu propósito, retendo-os apenas o tempo necessário para o atingimento desse desiderato. Assim, quaisquer políticas desposadas por controladores que busquem reter todo e qualquer tipo de informação do titular, sejam elas ou não pertinentes com a finalidade econômica do negócio jurídico havido entre eles, possivelmente será considerada ilícita.

O conceito de minimização pode ser depreendido da decisão prolatada pelo STJ[5] acerca do sistema "*credit scoring*" com prática comercial lícita (autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 - lei do cadastro positivo) porquanto destinada a desenvolver método para avaliação do "risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito)". O *credit scoring* é, basicamente, a reunião de variadas informações pelo controlador, oriundas de diferentes fontes, sobre o comportamento do titular quanto ao cumprimento de suas obrigações pecuniárias de modo e conceder-lhe uma "nota" a qual lhe qualificará no sistema de crédito (BRANCHER; BEPPU, 2019, p.136). Está na natureza do sistema de *credit scoring* a "maximização" das informações do titular pelo controlador, alcançando mesmo uma feição histórica e muito além da estreita natureza da relação jurídica especificamente havida com o titular, de forma a permitir ao controlador uma ampla avaliação acerca do comportamento pretérito do titular em face a suas obrigações pecuniárias.

[5] RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL.
I - TESES: 1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito).
2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo).
3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n.12.414/2011.
4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas.
5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.
II - CASO CONCRETO: 1) Não conhecimento do agravo regimental e dos embargos declaratórios interpostos no curso do processamento do presente recurso representativo de controvérsia; 2) Inocorrência de violação ao art. 535, II, do CPC.
3) Não reconhecimento de ofensa ao art. 267, VI, e ao art. 333, II, do CPC.
4) Acolhimento da alegação de inocorrência de dano moral "in re ipsa".
5) Não reconhecimento pelas instâncias ordinárias da comprovação de recusa efetiva do crédito ao consumidor recorrido, não sendo possível afirmar a ocorrência de dano moral na espécie.
6) Demanda indenizatória improcedente.
III - NÃO CONHECIMENTO DO AGRAVO REGIMENTAL E DOS EMBARGOS DECLARATÓRIOS, E RECURSO ESPECIAL PARCIALMENTE PROVIDO.
(REsp 1419697/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/11/2014).

Não obstante a autorização para a prática de *credit scoring* dada pela decisão referida, o mesmo julgado ressalva que, em tese, se configurado o "abuso de direito" no exercício do *credit scoring*, caberá ação de responsabilidade civil solidária contra o fornecedor do serviço, o responsável pelo banco de dados, da fonte e do consulente, não com base na LGPD, mas sim na Lei.12.414/2001 (lei do cadastro positivo).

Também no sentido de minimização e proporcionalidade no tratamento de dados, decidiu o STJ[6] que determinada cláusula inserida em contrato de cartão de crédito é "abusiva e ilegal" quando "autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento".

[6] RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE.
1. É facultado ao Juízo proferir sua decisão, desde que não haja necessidade de produzir provas em audiência, assim como, nos termos do que preceitua o princípio da livre persuasão racional, avaliar as provas requeridas e rejeitar aquelas que protelariam o andamento do processo, em desrespeito ao princípio da celeridade.
2. A Anadec - Associação Nacional de Defesa do Consumidor, da Vida e dos Direitos Civis tem legitimidade para, em ação civil pública, pleitear o reconhecimento de abusividade de cláusulas insertas em contrato de cartão de crédito. Precedentes.
3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento.
4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança.
5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada.
6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição.
7. Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão.
8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez que dita providência encontra amparo em lei (Lei n. 8.078/1990, arts. 43 e 44).
9. A orientação fixada pela jurisprudência da Corte Especial do STJ, em recurso repetitivo, no que se refere à abrangência da sentença prolatada em ação civil pública, é que "os efeitos e a eficácia da sentença não estão circunscritos a lindes geográficos, mas aos limites objetivos e subjetivos do que foi decidido, levando-se em conta, para tanto, sempre a extensão do dano e a qualidade dos interesses metaindividuais postos em juízo (arts. 468, 472 e 474, CPC e 93 e 103, CDC)" (REsp 1.243.887/PR, Rel. Ministro LUIS FELIPE SALOMÃO, CORTE ESPECIAL, DJe de 12/12/2011).
10. É pacífico o entendimento no sentido de que a revisão da multa fixada, para o caso de descumprimento de ordem judicial, só será possível, nesta instância excepcional, quando se mostrar irrisória ou exorbitante, o que, a meu ver, se verifica na hipótese, haja vista tratar-se de multa diária no valor de R$10.000,00 (dez mil reais).
11. Recurso especial parcialmente provido.
(REsp 1348532/SP, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 10/10/2017, DJe 30/11/2017).

Ao considerar que a obrigação anunciada pela cláusula contratual se "mostra prescindível à execução do serviço contratado", o STJ está indiretamente aplicando o princípio da necessidade e seu subsistema de proporcionalidade a medida em que o acórdão afirma que o contrato de prestação de serviços de cartão de crédito não mantém nenhuma relação de pertinência com a "necessidade" do consumidor autorizar o banco contratante a compartilhar dados com outras entidades financeiras e entidades mantenedoras de cadastros positivos e negativos de consumidores.

Pode-se dizer, também, que o princípio da minimização de dados está intimamente ligado a finalidade perseguida pelo tratamento: é em função desta(s) finalidade(s) que será possível mensurar se os dados coletados são, ou não, proporcionais.

### 1.2. Limitação no tempo

Os dados tratados deverão ser eliminados após o término de seu tratamento "no âmbito e nos limites técnicos das atividades" (art. 16 da LGPD), ou seja, os dados só poderão ser utilizados durante o período não excedente aquele necessário para atender a(s) finalidade(s) para as quais foram tratados. Trata-se de mais uma expressão da eficácia do princípio da minimização dos dados e da proporcionalidade no seu uso.

Nenhuma duração é fixada no texto legal. Determinar essa duração é uma questão pontual, caso a caso, sendo necessário definir, primeiramente, seu ponto de partida e os objetivos da coleta dos dados (MACHADO; BRUNO, 2016, p.355). É certo, porém, que o disposto no art. 16 da LGPD autoriza a manutenção dos dados para o cumprimento de obrigação legal ou regulatória pelo controlador, estudo por órgão de pesquisa, garantida, sempre que possível a anonimização dos dados, transferência à terceiros (respeitados os requisitos de tratamento de dados dispostos na lei) e para uso exclusivo do controlador, caso em que é vedado seu acesso por terceiros, e desde que anonimizados os dados.

Caberá ao controlador definir o ponto de partida da obtenção e conservação dos dados tratados. Ainda assim, é possível antever determinadas situações e a aplicação de princípios gerais.

Inicialmente, se a pessoa cujos dados pessoais são tratados mantém uma relação jurídica continuativa com o controlador (relação de trabalho, relação comercial, em especial na hipótese de contratos de trato sucessivo), será lógico considerarmos que os dados podem ser conservados

ao longo da duração de toda a relação. Nessas situações, o ponto de partida para o prazo de eliminação dos dados não será a data da sua coleta, mas sim a data do final da relação.

Como regra geral, o ponto de partida da duração da conservação dos dados corresponderá a um evento específico, não diretamente vinculado ao livre arbítrio do controlador, mas sim ligada a um ato jurídico. Assim, o ponto de partida corresponderá, como regra geral:

a) ao fim da relação jurídica havida entre o controlador e o titular dos dados;

b) nas situações em que não haja uma relação jurídica, a data da coleta.

Ainda assim é difícil afirmar até quanto os dados podem ser mantidos pelo controlador após o término da relação jurídica entres as partes. Por exemplo, numa compra em parcelas, é certo que o titular mantém sua relação com o controlador até o pagamento da última parcela devida, mas, de outro lado, a manutenção dos dados poderá ser uma necessidade para atender aos legítimos interesses do controlador (art. 7º, IX), sendo incerta a fixação do prazo de duração dos dados do titular em mãos do controlador em cadastro próprio.

Assim, em inúmeros casos, caberá ao controlador definir a duração da conservação dos dados por ele tratados em função de seu "legítimo interesse". Entretanto, tal definição deverá ser determinada pelo subprincípio da proporcionalidade, a partir de um critério intrínseco definidor das necessidades atribuídas ao tratamento, mas também tendo em conta os critérios extrínsecos resultantes das normas legais.

Há alguns critérios extrínsecos que podem ser analisados:

**a) A duração fixada por norma legal**

Um primeiro critério poderá ser fixado a partir da existência de norma legal que imponha uma duração de conservação para certos documentos ou informações. Cita-se, como exemplo, o disposto no art. 7º, X da lei 12.965/14 (Marco Civil da Internet) que determina a "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstos nesta Lei".

A LGPD, por sua vez, define no disposto em seu art. 15 quatro hipóteses de determinação do final da duração do tratamento de dados pessoais, a saber: a) o alcance da finalidade ou a constatação de que os dados deixaram de ser necessários para a finalidade desejada; b) fim do período de tratamento; c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; d) determinação de autoridade nacional, quando houver violação ao disposto na LGPD.

**b) A duração resultante de regulamento**

Nos termos da LGPD, caberá a Autoridade Nacional de Proteção de Dados – ANPD, conforme disposto art. 55 – J, inciso III "elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade" e, conforme inciso XX, "deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos".

Assim, há competência legal em favor da autoridade nacional para fixação de norma regulamentar destinada a normatizar a duração da conservação dos dados. Entretanto, em face da ausência de regulamentação, o controlador é livre para determinar a duração que ele considerar adequada às finalidades do tratamento.

O princípio da minimização e a proporcionalidade também devem ser observados sobre certos tratamentos que, em razão da natureza dos dados, e independentemente de sua finalidade, possam trazer consequências nefastas para seus titulares, e que por isso mesmo exigem um enquadramento legal ainda mais restrito.

Diga-se que o texto legal prevê três categorias de derrogações para o tratamento de dados pessoais, sendo a primeira aquele tratamento realizado por "pessoa natural para fins exclusivamente particulares e não econômicos" (art. 4º).

De outro lado temos a permissão para a conservação dos dados para fins jornalísticos, artísticos ou acadêmicos e, por fim, para questões exclusivas de "segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais."

A lei também trata dos "órgãos de pesquisa", assim definidos no art. 5º, XVIII, especificamente criados para a pesquisa de caráter "histórico, científico, tecnológico ou estatístico". Tais órgão têm permissão legal para o uso de dados pessoais sensíveis para fins de estudos (art. 11, *c*), além de conservá-los (para fins de estudos), desde que garantida e, em qualquer caso, garantindo, sempre que possível, a anonimização dos dados. Art. 16, II.

## 2. REGRAS ESPECIAIS À TRATAMENTOS ESPECÍFICOS

O princípio da minimização dos dados não se limita a equalização do conteúdo e extensão dos dados coletados e a finalidade do tratamento. O legislador também levou em consideração, de maneira absoluta e independente da finalidade da coleta, certos tratamentos de dados pessoais que, em razão de sua natureza, podem trazer consequências nefastas para seus titulares, e que por isso exigem um enquadramento mais restrito. Essas regras especiais

dizem respeito, de um lado, a tratamento sobre certas categorias de dados ditos “dados sensíveis” e, de outro, os tratamentos suscetíveis de criar riscos graves para seus titulares. Essas duas categorias de dados identificados pelo legislador como merecedores de uma proteção particular são os dados “sensíveis” (art. 11) e os dados que encerrem direitos fundamentais de “liberdade, de intimidade ou de privacidade”. (Art. 17).

### 2.1. O tratamento de dados sensíveis

A noção de “dados sensíveis” trazida pela LGPD necessita ser precisada. A LGPD define os dados sensíveis como sendo **“**dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (art. 5º, II).

A LGPD adota, assim, uma definição abrangente de “dados sensíveis”. A inclusão de dados genéticos ou biométricos nesse rol é importante, pois eles contêm informações únicas sobre o indivíduo que podem ser reveladas pelo seu tratamento, situação essa particularmente intrusiva na vida do cidadão e gerador de riscos específicos em caso de divulgação não autorizada. (BASTOS; ESTEVES, 2021, p. 237)

De fato, os dados sensíveis são suscetíveis de utilização para fins discriminatórios, como a estigmatização, exclusão ou segregação social, de modo a ferir a dignidade de seu titular. A própria natureza do conceito de dados sensíveis torna inviável concebê-los em rol taxativo, pois são definidos pelos efeitos potencialmente lesivos ao titular. Assim, a própria lei (art. 11, § 1º) determina a aplicação das regras relativas ao tratamento de dados sensíveis aos dados pessoais que, embora não sejam sensíveis por si sós, possam revelar-se, num dado contexto, como dados sensíveis. É o caso da localização geográfica do indivíduo, hábitos de compra, hábitos culturais e até mesmo histórico de pesquisa na internet, os quais podem parecer inofensivos isoladamente, mas cuja análise em conjunto poderá revelar a identificação política, religiosa e mesmo sexual do titular.

O TJRS[7] por sua vez, decidiu que dados empregados cotidianamente pelo cidadão (tais como CPF, endereço e outros) nas suas relações negociais não são dados considerados

[7] EMENTA: APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO COLETIVA. SPC BRASIL. MARKETING SERVICE. DIVULGAÇÃO DE DADOS. AUSÊNCIA DE OFENSA A DIREITOS DA PERSONALIDADE. HIPÓTESE EM QUE OS DADOS DIVULGADOS NÃO SÃO SIGILOSOS, POIS SE TRATA DE INFORMAÇÃO FORNECIDA NAS RELAÇÕES NEGOCIAIS COTIDIANAS. INEXISTÊNCIA

"sensíveis" e, portanto, podem até mesmo ser comercializados, posto que ausente proteção legal nesse sentido. Note-se que o julgamento data de 2016, portanto, antes da sanção (e vigência) da LGPD.

Por sua vez, os dados genéticos são aqueles de caráter pessoal relativos as características genéticas hereditárias ou adquiridas por um indivíduo, que dão informações únicas sobre sua fisiologia ou estado de saúde e que resultam, especialmente, da análise de uma amostra biológica da pessoa em questão.

Os dados genéticos se diferenciam dos dados relativos a saúde a medida em que estes revelam unicamente o estado de saúde em que a pessoa se encontra, enquanto aqueles permitem, quase sempre, identificar o indivíduo especificamente.

Já os dados sensíveis biométricos são definidos (BASTOS; ESTEVES, 2021, p. 225) como aquele conjunto de técnicas de informática que permitem reconhecer automaticamente um indivíduo a partir de suas características físicas, biológicas e comportamentais, ou seja, a partir de dados pessoais únicos e permanentes (DNA, impressão digital etc.). O uso de dados biométricos tende a crescer como alternativa eficaz em face de inúmeras e longas senhas de difícil memorização empregadas para uso de equipamentos eletrônicos.

Essa noção de dados biométricos está mais vinculada a uma modalidade técnica de tratamento do que a própria natureza dos dados. Do contrário, todos os atributos da pessoa (imagem, voz etc.) constituiriam "dados biométricos"[8]. Os dados pessoais biométricos

DE DADOS SENSÍVEIS. APELOS PROVIDOS. (Apelação Cível, Nº 70069420503, Sexta Câmara Cível, Tribunal de Justiça do RS, Relator: Ney Wiedemann Neto, Julgado em: 25-08-2016)

[8] Recentemente, a Justiça concedeu liminar ao Instituto Brasileira de Defesa do Consumidor (Idec) para que a Via Quatro, concessionária da Linha 4-Amarela do Metrô de São Paulo, interrompesse a coleta de "emoções" e reações dos usuários a estímulos publicitários, realizada a partir de sensores específicos instalados em outdoors eletrônicos ("portas interativas digitais") nas entradas dos vagões do metrô paulistano.

O que chama a atenção na ação civil pública ajuizada pelo Instituto em representação dos direitos dos usuários do metrô é que a petição inicial menciona os princípios e requisitos para tratamento de dados pessoais contidos na LGPD, que entrará em vigor apenas em agosto de 2020.

O instituto adota como fundamentos para a concessão da liminar as graves violações aos direitos à intimidade (art. 5º, X, CF/88), privacidade e à informação dos usuários do serviço público de mobilidade urbana e relaciona a coleta compulsória e utilização de dados pessoais sensíveis, sem o consentimento do usuário, a diversas violações a dispositivos do CDC, ao Marco Civil da Internet e ao Código de Defesa dos Direitos do Usuário dos Serviços Públicos. Segundo o Idec, a prática pode ser entendida como "uma pesquisa de opinião compulsória", o que configura abuso de direito, e a falta de informação clara, prévia e adequada quanto à coleta e tratamento de dados não atende a preceitos combinados expressos no CDC e no Marco Civil da Internet.

Em outro caso recente de suposto tratamento indevido de dados sensíveis, o Idec notificou a Hering para que a empresa preste esclarecimentos sobre o sistema de reconhecimento facial que, por meio de câmeras instaladas em uma loja conceito, permitiria à empresa "entender como os consumidores reagem às peças dispostas pela loja na medida em que, pela análise de expressões, é possível saber se os clientes gostam de determinado produto, além de traçar um perfil dos visitantes da loja, o que é interessante em tempos de hiperpersonalização". Complementarmente a esse sistema, noticiou-se que a loja possui sensores que registram

normalmente resultam de um tratamento técnico específico, relativo as características físicas, fisiológicas ou comportamentais de uma pessoa física que permita sua identificação, tais como imagens faciais ou dados datiloscópicos. A referência da lei a "tratamento de dados pessoais sensíveis ... genético ou biométrico" (art. 5º, II) sugere a necessidade de uso de recurso tecnológico, o qual poderá ser o critério caracterizador da natureza biométrica do tratamento.

Tratar dados sensíveis é, a princípio, proibido. Entretanto, esse princípio sofre exceções possíveis de agrupar em várias categorias diferentes:

**a)** o tratamento poderá ser fundado no consentimento específico e destacado do titular. O livre consentimento não poderá acarretar dano ao titular, ou seja, o consentimento só será entendido como "livre" se o titular não sofrer nenhuma sanção no caso de sua recusa. "Específico" significa que o consentimento deverá, justamente, referir-se a um determinado uso preciso de dados, com finalidades claras e determinadas;

**b)** Sem consentimento do titular, nas seguintes hipóteses:

**b.1)** cumprimento de obrigação legal ou regulatória pelo controlador;

A alínea respectiva (art. 11, II, a) repete o disposto no art. 7º, II, segundo o qual, em havendo determinação legal, o controlador poderá realizar o tratamento de dados pessoais com fundamento nessa base legal. A regra abrange apenas obrigação "legal ou regulatória". Obrigações contratuais não são alcançadas por essa norma. Não será possível ao controlador invocar relações privadas (contratuais) como fundamento para tratamento de dados pessoais.

**b.2)** tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

Essa exceção visa o tratamento necessário à execução de políticas públicas, em especial no campo da saúde pública em situações, por exemplo, onde haja ameaças de propagação de vírus letais ou mesmo para garantir o padrão das normas de qualidade e segurança nos cuidados médicos e medicamentos, sempre respeitada a dignidade do titular e o dever de guardar segredo profissional. Gize-se que a LGPD não é aplicável para fins exclusivos de segurança nacional, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III, a,b,c,d).

**b.3)** realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

---

ondas de calor conforme o interesse do consumidor nos produtos disponibilizados por toda a loja e produz um mapa com as áreas de maior interesse...." https://www.migalhas.com.br/depeso/301528/riscos-no-uso-indiscriminado-de-dados-biometricos Acesso em 20/05/2020.

É o caso de análises realizadas por institutos de pesquisa públicos ou privados para fins de estudos históricos, científicos e estatísticos. Entretanto, o uso desses dados deverá ser proporcional ao objetivo do estudo e sempre respeitada a essência do direito à proteção de dados. Em todos os casos devem ser previstas medidas apropriadas e específicas para salvaguardar os direitos fundamentais e interesses das pessoas envolvidas.

**b.4)** exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

Essa exceção diz respeito aos auxiliares da justiça e da própria jurisdição. Nada no texto legal limita o campo de aplicação da exceção às profissões judiciárias e jurídicas.

**b.5)** proteção da vida ou da incolumidade física do titular ou de terceiro;

Aqui a lei visa salvaguardar a vida humana. Essa "proteção" pressupõe o fato do titular ou terceiro estar incapacitado de dar seu consentimento. O fato poderá ocorrer, por exemplo, na hipótese de tratamento de dados sensíveis (de saúde) que exigiriam a autorização de uma pessoa gravemente ferida ou em estado de inconsciência.

**b.6)** tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

Aqui estamos diante dos tratamentos necessários para fins de medicina preventiva, de diagnósticos médicos, de administração de cuidados ou tratamentos médicos ou para pessoas às quais se imponha, em razão de suas funções, a obrigação de guardar segredo profissional.

**b.7)** garantia de prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Dados sensíveis podem ser tratados com o objetivo da prevenção à fraude e à segurança do titular como, por exemplo, em situações de tratamento de dados para acesso a locais restritos, para a realização de operações bancárias, para o combate a fraude em processos de identificação, entre outros. Todas as hipóteses exigem o emprego de sistemas eletrônicos (visando prevenir a fraude).

Não se encontra entre as exceções previstas no art. 11 da LGPD a questão dos dados tornados públicos pelo titular. Essa hipótese deve ser tratada com precaução. Ainda que seja possível ao controlador tratar os dados sensíveis do titular que os tenha voluntariamente tornados públicos, o controlador não poderá se utilizar desses dados simplesmente porque tenham sido coletados ou mesmo tornado públicos por um terceiro. Assim, por exemplo, um

órgão da imprensa que revela – licitamente – dados sensíveis descobertos em consequência de uma investigação, não autoriza o controlador a divulgá-los fora desse contexto.

Relativamente a dados infracionais ou condenatórios, o disposto no art. 17 determina que 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 da lei. Nada obstante essa regra, o tratamento de dados relativamente as condenações penais, infrações ou medidas de segurança, são considerados informações de ordem pública. Nesse sentido decide o TJRS[9].

O STJ[10], por seu turno, julgou que "é induvidoso o direito à preservação da privacidade e da intimidade, no que tange a divulgação de informações daquele sobre o qual recai o peso de

[9] EMENTA: CORREIÇÃO PARCIAL. INCONFORMIDADE DO MINISTÉRIO PÚBLICO. TRIBUNAL DO JÚRI. JUNTADA DE DOCUMENTOS DIVERSOS NOS AUTOS. DESENTRANHAMENTO.
1. Conforme entendimento já sedimentado em âmbito desta Colenda Terceira Câmara Criminal, informações alheias aos fatos denunciados no feito originário poderiam ensejar na produção de elementos paralelos para estigmatização do acusado ante o seu suposto envolvimento em delitos diversos. Precedentes. Nessa conjuntura, informações sobre a vida pregressa do acusado constituem argumento de autoridade, segundo interpretação hermenêutica do artigo 478 do Código de Processo Penal. Há diferença entre a juntada de Antecedentes Criminais e Informações extraídas do Sistema de Consultas Integradas. O primeiro - qualquer parte pode ter acesso, acusação ou defesa. Logo, trata-se de documentos de acesso público. O segundo, é de uso exclusivo somente a magistrados e ao órgão ministerial, não a defesa, seja Defensoria Pública ou defesa constituída. Portanto, trata-se de documentos de acesso restrito. Daí por que não há paridade de armas em permitir a juntada de documentos – Informações do Sistema de Consultas Integradas – que somente uma das partes tem acesso e a outra não, mas há paridade quando a juntada se trata de documentos cujo acesso é comum e possível a ambas as partes – Certidão de Antecedentes Criminais. Destarte, evidencia-se o prejuízo à defesa.
2. ....
CORREIÇÃO PARCIALMENTE PROCEDENTE. (Correição Parcial Criminal, Nº 70083709139, Terceira Câmara Criminal, Tribunal de Justiça do RS, Relator: Sérgio Miguel Achutti Blattes, Julgado em: 20-02-2020).

[10] RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA - EXCLUSÃO DE INFORMAÇÕES SOBRE CONDENAÇÃO CRIMINAL DO BANCO DE DADOS DO INSTITUTO DE IDENTIFICAÇÃO RICARDO GUMBLETON DAUNT - IIRGD - ART. 748 DO CPP - EXTINÇÃO DA PUNIBILIDADE - CUMPRIMENTO DA PENA - DIREITO À INTIMIDADE - ART. 202 DA LEP - PODER JUDICIÁRIO - ACESSO - POSSIBILIDADE - AUSÊNCIA DE PROVA PRÉ-CONSTITUÍDA - DILAÇÃO PROBATÓRIA - VEDAÇÃO - RECURSO ORDINÁRIO DESPROVIDO.
1 - As Turmas que compõem a Eg. Terceira Seção, entendem que, "por analogia à regra inserta no art. 748 do Código de Processo Penal, as anotações referentes a inquéritos policiais e ações penais não serão mencionadas na Folha de Antecedentes Criminais, nem em certidão extraída dos livros do juízo, nas hipóteses em que resultarem na extinção da punibilidade pela prescrição da pretensão punitiva, arquivamento, absolvição ou reabilitação." (RMS n. 29.423/SP, Rel.
Ministra Laurita Vaz, 5T, DJe 21.9.2011).
2 - É induvidoso o direito à preservação da privacidade e da intimidade, no que toca à divulgação de informações daquele sobre o qual recai o peso de uma condenação ou tão somente da obrigação de comparecer perante o Estado para responder a um processo criminal, mormente nos casos de extinção da punibilidade pela prescrição da pretensão punitiva, arquivamento, absolvição ou reabilitação.
3 - Se até a reabilitação, ainda que não superado o prazo de cinco anos para os fins de reincidência, previsto no art. 64, inc. I, do CP, é capaz de conferir sigilo aos assentos penais do acusado, desses não podendo nem a autoridade policial nem os serventuários da justiça fornecer certidão ou atestado senão por força de requisição judicial, o mesmo se dirá quanto aos casos de extinção da punibilidade pela prescrição e, muito mais, quanto aos casos de absolvição ou, seja qual for a motriz, de arquivamento de inquérito.
4 - Operada qualquer das hipóteses mencionadas, aparenta vício de ilegalidade o livre acesso aos Terminais de Identificação por agentes públicos que não o juiz criminal, visto que a Lei de Execuções Penais, bem como o

uma condenação... mormente nos casos de extinção da punibilidade pela prescrição da pretensão punitiva, arquivamento, absolvição ou reabilitação”**.** Nessas hipóteses, segundo o aresto citado, o Código de Processo Penal, atentos à disciplina do Código Penal, fixaram o caráter sigiloso das informações penais.

## CONCLUSÃO

O artigo visou trazer à exame a aplicação do princípio da minimização de dados e seu corolário legal, o subprincípio da proporcionalidade, presentes em diversos aspectos da LGPD. A proporcionalidade se faz presente na lei como forma e parâmetro de aplicação da minimização dos dados, inclusive para interpretação da limitação de conservação dos dados no tempo, os quais só poderão ser utilizados, como regra geral, durante o período não excedente aquele necessário para atender sua finalidade. A proporcionalidade também se faz presente quando a lei exige a “análise de impacto” a certos tratamentos de dados, seja em face do impacto e amplitude social que eles representam, seja pelo emprego de tratamento automatizado o qual, por si só, traz o perigo de criação de “perfis” falsos e tendenciosos do titular.

A minimização e proporcionalidade das informações visam garantir os direitos de personalidade do titular e conferir-lhe segurança jurídica. Caberá ao controlador realizar o teste da proporcionalidade dos dados coletados em face do tratamento a ser com eles realizado: quanto mais a natureza e a quantidade de dados pessoais forem proporcionais aos objetivos do tratamento, tanto mais o tratamento se reverá lícito e legítimo.

---

Código de Processo Penal, atentos à disciplina do Código Penal, fixaram o caráter sigiloso das informações penais acerca do reabilitado e daquele em favor de quem se tenha operado a extinção da punibilidade.
5 - Somente o juiz criminal, e para certos e determinados fins, a autoridade habilitada a determinar o acesso aos antecedentes penais daqueles protegidos pelo manto da reabilitação, da absolvição ou da extinção da punibilidade pela prescrição.
6 - Sendo possível ao juiz criminal requisitar tais dados dos arquivos no Poder Judiciário, não há razão para mantê-los em outros lugares, sob pena de conferir a guarda da presunção de inocência e da intimidade da pessoa humana a agentes de polícia, bancas examinadoras de concurso público e cartórios extrajudiciais.
7 - No mandado de segurança exige-se que todas as provas dos fatos alegados venham acompanhadas da exordial da ação, ante a consabida incompatibilidade desta via com o alargamento da dilação probatória.
8 - Na hipótese dos autos, ao pugnar pela exclusão das informações relativas ao processo criminal n. 050.04.027217-6, que tramitou na 20ª Vara Criminal da Comarca de São Paulo, o recorrente não juntou cópia de documentos comprobatórios da efetiva exposição desses dados em bancos outros que não o destinado ao acesso do Poder Judiciário, o que comprovaria o concreto prejuízo aventado, consistente na negativa de conseguir emprego, com a consequente exclusão do mercado de trabalho.
9 - Recurso ordinário a que se nega provimento.
(RMS 38.920/SP, Rel. Ministro ROGERIO SCHIETTI CRUZ, SEXTA TURMA, julgado em 07/11/2013, DJe 26/11/2013)

Por fim, não nos esqueçamos que o subprincípio da proporcionalidade também se faz presente no § 1º do art. 10[11], no art. 16[12] e no art. 18, VI[13], todos da LGPD, os quais restringem os dados coletados ao estritamente necessário para o cumprimento da finalidade informada.

Em suma, a proporcionalidade é um subprincípio fundamental a todas as atividades de processamento de dados, o qual indica a correlação necessária que deve existir entre a coleta e o uso dos dados pessoais e a finalidade comunicada aos interessados no momento desta coleta. A proporcionalidade serve como parametrização do uso dos dados pessoais como adequados e razoáveis aos fins a que se destina, considerando-se as premissas sob as quais os dados foram coletados junto aos titulares, sempre visando a defesa dos direitos fundamentais de privacidade, personalidade e dignidade do titular.

Não obstante as medidas de proteção de dados não estarem adstritas às previsões constitucionais (pois o avanço tecnológico trouxe um anova casuística), não há dúvidas de que o subprincípio da proporcionalidade tem raiz constitucional e destina-se a proteção dos direitos da privacidade e a efetivação dos incisos X e XII do art. 5º da Carta Magna que tratam da inviolabilidade da intimidade e da vida privada, bem como do sigilo de correspondência e comunicações telefônicas.

## REFERÊNCIAS

BARROS, Bruno M. Correa de.; BARROS, Clarissa T. Lovatto; OLIVEIRA, Rafael Santos de. O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais. **Revista Videre**, Dourados, MS, v.9, n.17. 1º semestre de 2017.

BASTOS, Elisio; ESTEVES, Vitoria B. **Revista Direitos Democráticos & Estado Moderno**. Faculdade de Direito da PUC-SP. DD&EM nº 03, p. 216-240, jul-dez. 2021.

BRANCHER, Paulo Marques Rodrigues; BEPPU, Ana Claudia. **Proteção de dados no Brasil. Uma nova visão a partir da lei nº 13.709/2018**. Belo Horizonte: Forum, 2019.

[11] Art. 10(...) § 1º. Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

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

[13] Art. 18. O titular de dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei: (...)

CRAVO, Daniela Copetti. **Direito a Portabilidade de Dados**. Rio de Janeiro, Lumen Juris, 2018.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**. Vol. 13/2017, p. 59-67. Out-Dez 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar. 2006.

FRAZÃO, Ana. **Tratamento de dados pessoas sensíveis**. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em 02/06/2022.

FREDES, Andrei; BORGES, Mariana. **Revista Direitos Democráticos & Estado Moderno. Faculdade de Direito da PUC-SP**. DD&EM nº 02, p.181-195, Jan-Jun.2021.

MASSO, Fabiano Del; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio. **Marco civil da internet.** Lei 12.965/14. São Paulo: Ed. Revista dos Tribunais. 2014.

MACHADO, Jorge; BIONI, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: Um estudo de caso no "Nota Fiscal paulista". **LIINC em Revista**, Rio de Janeiro, v. 12, n.2, p.350-364, novembro de 2016. http://www.oboct.br/liinc.

MARQUES, Claudia Lima; et al., **Manual de Direito do Consumidor.** São Paulo: Ed. RT, 2008.

MARQUES, Claudia Lima. **Contratos no código de defesa do consumidor**. 5ª ed. São Paulo: RT, 2006.

MARTINS, Guilherme Magalhães; LONGHI, João Vitor Rozatti. **Direito Digital**. São Paulo: RT, 2019.

MENDES, Gilmar. **Curso de direito constitucional**. 2ª ed. São Paulo: Saraiva, 2008.

MIRAGEM, Bruno. **A lei gral de proteção de dados (lei 13.709/2018) e o direito do consumidor.** Revista dos Tribunais on-line, São Paulo: vol. 1009/2019.

OPICE BLUM, Renato; MALDONADO, Viviane Nobrega. **Comentário ao GDPR.** São Paulo: RT, 2018.

OPICE BLUM, Renato; MALDONADO, Viviane Nobrega. LGPD **Lei Geral de Proteção de Dados. Comentário**. Ed. RT, SP-SP, 2019.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro, Renovar. 2008.

SARLET, Ingo Wolfgang. **Curso de Direito Constitucional**, 3ª ed, p. 400. Ed. RT. SP-SP, 2013.

TEPEDINO, Gustavo. **A tutela da personalidade no ordenamento civil - constitucional brasileiro**. 2004, Renovar.

TEPEDINO, Gustavo; FRAZAO, Ana e OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil-constitucional_brasileiro. Acesso em 02/06/2022.

Recebido – 02/12/2021
Aprovado – 14/06/2022