A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI 13.709/2018) E A SUA PRINCIPIOLOGIA

The Brazilian General Data Protection Law (Law 13,709/2018) and its principiology

Revista dos Tribunais | vol. 1027/2021 | p. 203 - 243 | Maio / 2021
DTR\2021\7888

Guilherme Magalhães Martins
Doutor e Mestre em Direito Civil pela Faculdade de Direito da UERJ. Professor permanente do Doutorado em Direito, Instituições e Negócios da Universidade Federal Fluminense. Professor associado de Direito Civil da Faculdade Nacional de Direito – Universidade Federal do Rio de Janeiro. Promotor de Justiça titular da 5ª Promotoria de Tutela Coletiva do Consumidor e do Contribuinte – Ministério Público do Estado do Rio de Janeiro. gui_mart@terra.com.br

Área do Direito: Civil; Digital
Resumo: A importância dos direitos da personalidade, e a necessidade de sua proteção, refletiu-se em diversos sistemas jurídicos, notadamente após a segunda grande guerra, por outorgar autonomia não apenas física, mas também moral, particularmente da condução da sua vida, na autoatribuição de fins a si mesmo, na eleição, criação e assunção da sua escala de valores, na prática de seus atos, na reavaliação deles e na recondução do seu comportamento. Sob essa perspectiva, um dado, atrelado à esfera de uma pessoa, pode se inserir entre os direitos da personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular. Com base nisso, essa pesquisa se dedicará à análise do rol de princípios que inspirou a Lei Geral de Proteção de Dados, tomando como pressuposto a revisão dos temas que levaram o legislador a editá-lo. Pelo método dedutivo, a pesquisa se baseará em análise bibliográfica e, ao final, procurar-se-á extrair conclusão assertiva acerca do tema.

Palavras-chave: Proteção de dados – Princípios – Relações de consumo
Abstract: The importance of personality rights, and the need for their protection has been seen in several legal systems, notably after the Second World War, for granting not only physical but also moral autonomy, particularly in the autonomy to conduct their lives, in the self-attribution of ends, in the election, creation and assumption of its scale of values, in the practice of its acts, in the reevaluation of them and in the renewal of its behavior. From this perspective, data, linked to a person's sphere, can be inserted among the rights of the personality. For this, it must be defined as personal, characterizing itself as a projection, extension or dimension of its holder. Based on this, this research will be dedicated to the analysis of the principles that inspired the Brazilian General Data Protection Law, assuming the revision of the themes that led the legislator to edit it. By the deductive method, the research will be based on bibliographic analysis and, in the end, it will try to extract an assertive conclusion about the theme.

Keywords: Data protection – Principles – Consumer relations

Para citar este artigo: MARTINS, Guilherme Magalhães. A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e a sua principiologia. *Revista dos Tribunais.* vol. 1027. ano 110. p. 203-243. São Paulo: Ed. RT, maio 2021. Disponivel em: inserir link consultado. Acesso em: DD.MM.AAAA.

Sumário:

1. Introdução

A importância dos direitos da personalidade, e a necessidade de sua proteção, refletiu-se em diversos sistemas jurídicos, notadamente após a segunda grande guerra. Ainda em 1948, a Declaração Universal de Direitos Humanos, em seu art. I previu: "Todas as pessoas nascem livres e iguais em dignidade e direitos". A mesma Declaração Universal, em seu art. XII, assegurou que nenhuma pessoa poderia ser "sujeito a interferências na sua vida privada", ou de ofensas "à sua honra e reputação"[1].

Essa premissa irradiou-se em diversos sistemas jurídicos, e o Brasil adotou a proteção constitucional de direitos da personalidade, a partir da cláusula geral da dignidade da pessoa humana, explicitada no artigo 1º, III, da Constituição de 1988 como um dos fundamentos da República Federativa do Brasil.[2]

Da cláusula geral da dignidade humana – em face da qual não há que se discutir sobre uma enumeração taxativa ou exemplificativa dos direitos da personalidade –, irradiam-se a privacidade[3], a honra, a imagem, a identidade pessoal, a proteção de dados pessoais, entre outros atributos da pessoa. No desenvolvimento da personalidade, releva, ainda, o poder de autodeterminação do seu titular. Desde logo, na escolha de finalidades ou objetivos, no recolhimento de informações e no empreendimento de ações, assim como na abertura a terceiros dos seus dados pessoais.[4]

A dignidade humana, portanto, outorga autonomia não apenas física, mas também moral, particularmente da condução da sua vida, na autoatribuição de fins a si mesmo, na eleição, criação e assunção da sua escala de valores, na prática de seus atos, na reavaliação deles e na recondução do seu comportamento.[5]

Sob essa perspectiva, um dado, atrelado à esfera de uma pessoa, pode se inserir entre os direitos da personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular.[6]

Nesse sentido, cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e se movimentam a partir desses signos identificadores do cidadão. Trata-se de um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações.[7]

Os dados pessoais têm sido utilizados por governos e grandes *players* econômicos para a criação de um *one-way mirror,* possibilitando que tais agentes saibam tudo dos cidadãos, enquanto estes nada sabem dos primeiros. Isso acontece por meio de um monitoramento e vigília constantes sobre cada passo da vida das pessoas, levando a um capitalismo de vigilância, cuja principal consequência é a constituição de uma sociedade também de vigilância.

Segundo Bruno Bioni, isso acaba por identificar dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade, assegurando, por exemplo, que uma pessoa exija a retificação dos seus dados pessoais para que a sua projeção seja precisa. Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes dos direitos à privacidade e à intimidade. O eixo da privacidade está ligado ao controle de informações pessoais de algo interno ao sujeito. A proteção dos dados pessoais pode estar sob a esfera pública, discutindo-se, apenas, a sua exatidão, por exemplo.[8]

A Constituição Federal brasileira, em seu art. 5º, ao tratar dos Direitos e Garantias Fundamentais, traz um inciso específico (o inciso X) para instituir a inviolabilidade da intimidade, da vida privada, honra e imagem da pessoa (reproduzida no art. 7º, I, do Marco Civil da Internet – MCI, Lei 12.965/2014 (LGL\2014\3339))[9]. Já inciso XII do mesmo artigo explicita a inviolabilidade da correspondência, de dados e comunicações.

Não obstante esse inciso X tratar, ao final de seu texto, especificamente da tutela indenizatória, é possível verificar que a Constituição Federal atribuiu extrema relevância e instituiu extensa proteção aos referidos direitos de personalidade.

Da mesma forma, estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada um direito fundamental autônomo, mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade, ensina Stefano Rodotà.

A Carta de Direitos Fundamentais da União Europeia, em 2000, reconheceu a proteção de dados como um direito autônomo. Esse pode ser considerado o último ponto de uma longa evolução, separando a privacidade da proteção de dados. A proteção de dados encontra-se ligada ao *corpo eletrônico* da pessoa humana, tratado no artigo 8º da Carta[10], em contraposição ao *corpo físico,* ligado à integridade da pessoa (artigo 3º).[11]

A União Europeia, por intermédio do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, introduziu alterações importantes sobre a proteção da pessoa humana no tratamento de dados pessoais, em especial sobre os dados sensíveis, que, independentemente do formato com que são coletados, impõem novas obrigações aos cidadãos e a todas as instituições, públicas e privadas, ao exigir a adoção de medidas técnicas e organizativas adequadas.[12]

Ao mesmo passo que os provedores desenvolvem ferramentas e aplicações cada vez mais sofisticadas para a captação dos dados e categorização dos consumidores, pressionam para que a legislação os isente de promover a tutela da personalidade dos usuários.

Nos últimos anos temos assistido um aumento de preocupação na esfera pública relativo à tutela jurídica do direito fundamental à proteção de dados pessoais, cuja autonomia se impõe, na exata medida em que a informação se tornou a substância essencial da composição de uma nova morfologia estruturante da sociedade.

Salvaguardas não deveriam ser baseadas em princípios que consideram o indivíduo somente como dono dos dados a seu respeito. A implementação desse direito fundamental implica o esvaziamento de qualquer visão patrimonialista, visto que o direito à proteção de dados se refere à proteção da personalidade, e não da propriedade.[13]

Isso implica considerar que os dados pessoais chegam a fazer as vezes da própria pessoa. E, nesse cenário, o tratamento de tais dados adquire notável relevância, a ponto de se definir a proteção constitucional para as informações e para os dados pessoais.

2. Dados pessoais e consumo: panorama da LGPD

Os dados pessoais se destacam cada vez mais como um ativo na economia da informação, com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo ("marketing") e sua promoção. Isso se deve à sua utilização por governos e grandes *players* econômicos para que esses saibam tudo dos cidadãos-usuários, enquanto esses nada sabem dos primeiros.

E tudo isso acontece por meio de um monitoramento e vigília constantes sobre cada passo na vida das pessoas, o que leva a um verdadeiro capitalismo de vigilância.

Por um outro lado, a evolução da chamada sociedade da informação impôs aos Estados um dever, consubstanciado na "promoção de um equilíbrio entre os valores em questão, desde as consequências da utilização da tecnologia para o processamento de dados pessoais, suas consequências para o livre desenvolvimento da personalidade, até a sua utilização pelo mercado".

Da mesma forma, o Marco Civil da Internet, Lei 12.965/2014 (LGL\2014\3339), art. 3º, reconhece como princípio da disciplina do uso da Internet, lado a lado com a proteção da privacidade (inciso II), a proteção aos dados pessoais, na forma da lei (inciso III).

A partir dessa constatação inicial, verifica-se que existe, sob um enfoque preliminar e puramente apriorístico, uma prevalência dos interesses relacionados aos direitos de personalidade sobre outros que não estejam em um mesmo patamar de importância. Em outras palavras, as situações jurídicas existenciais devem sempre prevalecer sobre as patrimoniais.

Embora possa haver conflitos entre duas ou mais situações jurídicas subjetivas, cada uma delas amparada por um desses princípios, logo conflito entre princípios de igual importância hierárquica, o fiel da balança, a medida da ponderação, o objetivo a ser alcançado, já está determinado, *a priori,* em favor do conceito da dignidade humana.[14]

Na Comunidade Europeia, a Carta de Direitos Fundamentais prevê não somente um direito autônomo, pois também consagra os princípios do consentimento e da finalidade da coleta e do processamento de dados com *status* normativo diferenciado, além de prever, no plano do direito fundamental, a necessidade de uma autoridade *independente* para a aplicação de sanções nesse caso.

O Regulamento 2.016/679, denominado "Regulamento Geral sobre Proteção de Dados" – RGPD –,

por sua vez, foi pioneiro em reforçar e tornar mais próximos da realidade atual institutos considerados avançados, como o direito a deletar dados, o direito ao esquecimento, o direito à portabilidade de dados pessoais, além de conter normas que vão além das já estabelecidas autoridades de proteção de dados em cada um dos países, disciplinando o Comitê Europeu de Proteção de Dados.

O ordenamento jurídico brasileiro contava com menções à proteção de dados no Marco Civil da Internet (Lei 12.965/14 (LGL\2014\3339) – MCI), mas apenas em 2018 aprovou a Lei Geral de Proteção de Dados (Lei 13.709/18 (LGL\2018\7222) – LGPD). [15]

A lei brasileira é expressão da convergência internacional em torno de princípios básicos da proteção de dados pessoais no mundo, ensejando uma aproximação entre as diversas normas, em conteúdo e forma, para além das peculiaridades nacionais, trazendo consigo a identidade de um padrão normativo entre os diversos sistemas internacionais.

A versão original da Lei de Proteção de Dados Pessoais foi marcada inicialmente pelos vetos, especialmente à criação da Agência Nacional de Proteção de Dados e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (respectivamente, nos artigos 55 e 58 do projeto de lei aprovado pelo Senado Federal e vetados pela Presidência da República).

À Agência Nacional de Proteção de Dados caberia o papel de "autoridade garante", como a famosa "*Garante Privacy*" italiana, já presidida pelo jurista Stefano Rodotà – algo que já foi sinalizado pelo Governo que será resolvido por lei de iniciativa privativa do Presidente da República.

Apesar dos vetos, não pode ser desmentido o indiscutível avanço trazido pelo texto inicial da LGPD em relação ao direito anterior, do ponto de vista da promoção da personalidade humana.

Em dezembro de 2018, o governo Michel Temer editou a Medida Provisória 869/2018 (LGL\2018\12628), que já traz alterações ao texto da LGPD, entre elas uma dilatação do prazo de *vacatio legis*, aumentando ainda mais o lapso para sua entrada em vigor no tocante à matéria da proteção de dados (art. 65, inciso II), que passa a ocorrer em agosto de 2020.

Posteriormente, num terceiro momento, tendo sido realizadas diversas audiências públicas e realizados intensos debates acerca das alterações, foi promulgada a Lei 13.853, de 08 de julho de 2019 (LGL\2019\5777), que manteve alguns dos ajustes realizados, efetivou outros e recompôs o texto original em certos pontos.

A Lei 13.853/2019 (LGL\2019\5777) introduziu os artigos 55-A a 55-L, que consideram a Autoridade Nacional de Proteção de Dados (ANPD)[16], órgão da administração pública federal, integrante da Presidência da República.(art. 55-A), com natureza transitória podendo ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República (art. 55-A, parágrafo primeiro).

O Artigo 55-C disciplina os órgãos componentes da Autoridade Nacional de Proteção de Dados, a saber: I – o Conselho Diretor, órgão máximo de direção; II – o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III – a Corregedoria; IV – a Ouvidoria; V – o órgão de assessoramento jurídico próprio; e VI – unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei."

A nova legislação se contrapõe à Lei Complementar 866, de 8.4.2019, que torna obrigatória a participação de todos os consumidores no cadastro positivo, alterando diversos dispositivos da Lei 12.414, de 9 de junho de 2011 (LGL\2011\1883).

O objetivo da Lei Complementar é dar todo poder aos gestores de cadastros, publicizando e compartilhando obrigatoriamente as informações de adimplemento das pessoas naturais e jurídicas, que passam a ser rotuladas com uma nota ou "score", agora por imposição legal.[17] Não se pode olvidar que a proteção ao crédito, na forma da legislação pertinente, é ressalvada pelo artigo 7º, X, da LGPD como exceção à regra do consentimento do titular para o tratamento de dados pessoais.

Em seu artigo 2º, a Lei Geral de Proteção de Dados estabelece como fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o direito ao livre

desenvolvimento da personalidade, o desenvolvimento econômico e tecnológico, a livre-iniciativa, a livre concorrência e a defesa do consumidor.

Alguns outros pontos da Lei de Proteção de Dados pessoais merecem ser mencionados.

Primeiramente, as exceções previstas no art. 4º, com destaque para termos genéricos como "segurança pública", "defesa nacional", "investigação e repressão de infrações penais" etc., aos quais a lei remete à legislação específica. Em que pese a exceção, segue a normativa constitucional e as regras da "reserva de jurisdição" etc.

Segundo, os conceitos trazidos no art. 5º.

A LGPD, seguindo a linha de outros sistemas jurídicos, qualifica os dados pessoais como as informações relacionadas a uma pessoa natural identificada ou identificável, no inciso I do artigo 5º.

Destacam-se ainda os dados sensíveis, cuja doutrina sempre salientou a necessidade de regime jurídico especial; tratamento de dados, definindo a atividade dos agentes que se submetem às regras e às sanções da lei. A lei os define (artigo 5º, II) como dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além daqueles referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Ainda no artigo 5º, deve ser enfatizado o contraponto entre os controladores – definidos no inciso VI como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais – e os operadores, que realizam o tratamento de dados pessoais em nome dos controladores (inciso VII).

Outro aspecto fundamental diz respeito ao consentimento como ponto de partida para o processamento de dados pessoais. A proteção de dados pessoais ganha autonomia em relação à privacidade, à honra, à identidade pessoal e à imagem, de modo que, considerando-se a esfera privada como um conjunto de ações, comportamentos, preferências, opiniões e comportamentos pessoais sobre os quais o interessado pretende manter um controle exclusivo, essa tutela pressupõe uma autodeterminação informativa.

É o que determina o artigo 7º, que estabelece como regra para o tratamento de dados pessoais o consentimento do titular, no seu inciso I. Fica dispensado o consentimento em hipóteses estritas, como o cumprimento de obrigação legal ou regulatória pelo controlador (inciso II), o tratamento compartilhado de dados necessários à execução de políticas públicas pela administração pública (inciso III), a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados sensíveis (inciso IV), quando necessário para a execução de contrato ou de procedimentos preliminares a esses relacionados (inciso V), para o exercício regular de direitos, em processo judicial, administrativo ou arbitral (inciso VI), para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII), para a tutela da saúde (inciso VIII) ou quando necessário para atender aos interesses legítimos do controlador ou do terceiro (inciso IX).

Afinal, trata-se da autonomia para a construção da proteção de dados, ou seja, do poder de controle sobre quem, quando e como serão esses exercidos.

Eis a razão de ser do artigo 15 e seguintes, com regras sobre o término do tratamento dos dados pessoais.

Sobre os direitos do titular dos dados, merece destaque a possibilidade de revogação do consentimento: afinal, a disponibilidade das situações existenciais integra a liberdade integrante da noção de dignidade humana, pois sempre é possível mudar de ideia.

A Lei de Proteção de Dados coloca em primeiro plano a pessoa humana, ou seja, o titular de dados pessoais, que tem reconhecidos seus direitos, no artigo 18, em especial: à confirmação da existência de tratamento (inciso I); ao acesso aos dados (inciso II); à correção de dados incompletos, inexatos ou desatualizados (inciso III); à anonimização, ao bloqueio ou à eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na mesma lei (inciso IV); à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos

comercial e industrial (inciso V); à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei (inciso VI); à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (inciso VII); à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; à revogação do consentimento, nos termos do § 5º do artigo 8º da Lei (inciso IX).

Destaca-se ainda o direito de o usuário requisitar seus dados independentemente de judicialização, tendência louvável se comparada ao Marco Civil da Internet no regime de responsabilidade dos provedores por conteúdo inserido por terceiros, condicionada à difícil via judicial.

No que tange aos regimes especiais, a lei traz regras específicas sobre o tratamento de dados de crianças e adolescentes e aponta diretrizes na conduta do poder público fora das situações excepcionais do art. 3º.

A LGPD, em seu artigo 42, *caput,* adota um regime de responsabilidade civil objetiva dos controladores ou operadores que, em razão do exercício ou atividade de tratamento de dados pessoais, causarem a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais. Tal dispositivo inclusive revoga o art. 19 do Marco Civil da Internet, caso o provedor de aplicações Internet funcione igualmente como controlador ou operador em relação aos dados pessoais dos usuários.

As possíveis excludentes de responsabilidade seguem contempladas no artigo 43 da LGPD.[18]

O artigo 44 da LGPD, de forte inspiração consumerista, estabelece que

"O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I – o modo pelo qual é realizado;

II – o resultado e os riscos que razoavelmente dele se esperam;

III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado."

Já a Lei 13.853/2019 (LGL\2019\5777) alterou o conceito de "encarregado" (art. 5º, VIII), que, antes, deveria ser uma pessoa natural. Agora, permitiu-se que tal função seja realizada por tratamento automatizado de dados, regido pelos mesmos algoritmos que dão ensejo ao que Frank Pasquale denomina "Sociedade da caixa preta".[19]

A Lei 13.853/2019 (LGL\2019\5777) retrocedeu em relação à redação original da Lei 13.709/18 (LGL\2018\7222) ao alargar as exceções ao sistema geral de proteção dos dados sensíveis, baseado, em última análise, no consentimento informado, acrescendo ao artigo 11 no § 4º.

O novo § 4º do artigo 11 prevê:

"É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I – a portabilidade de dados quando solicitada pelo titular; ou;

II – as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo."

No tocante aos dados do Poder Público (artigo 26, § 1º), fez o mesmo, alargando o rol de exceções e facilitando, por conseguinte, seu fluxo fora das hipóteses em que há consentimento do cidadão, dispensando-se também da comunicação por parte do Poder Público nessas hipóteses (art. 27).

Mas o principal aspecto do texto da Lei 13.853/2019 (LGL\2019\5777) é a criação da Autoridade Nacional de Proteção de Dados e do Conselho Nacional (arts. 55-A e ss.), objetos de veto

presidencial no texto original da lei, não obstante fundamental para a efetividade dos direitos fundamentais ali previstos.

A partir da visão das mais de 40 hipóteses do texto legal em que a Autoridade é chamada a atuar, sua competência é ampla, abrangendo desde a solicitação e a análise de relatórios de impacto de privacidade, determinação de medidas para reverter efeitos de vazamentos de dados, disposição sobre padrões técnicos de segurança da informação e até mesmo a autorização para a transferência internacional de dados pessoais.

Mais do que um mero coadjuvante, trata-se do arcabouço normativo e principiológico do novo sistema, ainda que integrado com outras fontes, como o Código Civil (LGL\2002\400), o Código de Defesa do Consumidor e o Marco Civil da Internet.

É inegável que a ideia de um direito autônomo à proteção dos dados pessoais surge relacionada ao controle de acesso, que restringe quem pode visualizar determinado conteúdo, assegurando-se aos indivíduos que produzem ou influenciam informações relacionadas a si mesmos o direito de determinar as permissões (de acesso e até de compartilhamento) que desejam conceder a outrem, mas, também, sanções e mecanismos de controle e fiscalização – funções da ANPD. Tratava-se de ausência sentida, na medida em que a lei trouxe inúmeras menções à Agência Nacional, em seu texto original, ao modelo de outros países, como forma de regulamentar e fiscalizar a concretização de tal direito fundamental na contemporaneidade.

A autoridade, no texto vetado, seria uma autarquia especial, vinculada ao Ministério da Justiça, com independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira (art. 55 *caput* e § 3º), o que inegavelmente era visto com bons olhos.

De início, a reforma acrescentou ao artigo 1º um parágrafo único, com a seguinte redação: "As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios." Trabalhou-se, conceitualmente, com a concretização da amplitude axiológica do direito fundamental à proteção de dados pessoais[20], alinhando-a ao que se discute na Proposta de Emenda à Constituição 17/2019, que visa incluir tal direito no texto constitucional, além de definir como de competência exclusiva da União o poder para legislar sobre o assunto.

Sem dúvida, o *status* de direito fundamental confere à proteção de dados pessoais um papel imprescindível no tocante à articulação do direito privado diante dos interesses passíveis de tutela no contexto informacional[21].

Nessa esteira, o acréscimo normativo ainda deixa mais clara a incidência dos dispositivos da lei aos afazeres e às atividades do Poder Público, proclamando a obrigatoriedade de sua observância em todos os âmbitos.

Avançando, nota-se que, no sentido de tornar mais preciso o texto da LGPD, foi mantida pela Lei 13.853/19 (LGL\2019\5777) a redação dada pela MP 869 ao artigo 3º, inciso II, da Lei. O objeto da referida mudança foi simplesmente a inserção da conjunção "ou" ao final de seu texto (consolidado como "a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou") para não haver dúvida alguma de que o âmbito de aplicação da lei não ostenta requisitos cumulativos, mas alternativos, nas hipóteses descritas pelos três incisos do artigo 3º da Lei[22].

Outro aspecto fundamental da reforma pertine aos dados acadêmicos, excetuados pela MP 869 do alcance da LGPD (artigo 4º, inciso II, "b"), mas que a Lei nº 13.853 acabou por reformular, retomando a redação originalmente aprovada no texto original anterior à MP.

Ao artigo 4º, § 4º, que, até então, enunciava apenas que "[e]m nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do *caput* deste artigo poderá ser tratada por pessoa de direito privado", foi inserida uma ressalva: "salvo por aquela que possua capital integralmente constituído pelo poder público." Nota-se, à toda evidência, uma flexibilização do campo regulatório da norma, que, por força do mencionado inciso III, afasta de seu escopo de incidência o tratamento de dados realizado para fins de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais.

Com a nova redação dada ao § 4º, a mesma liberdade de tratamento de dados passa a valer para pessoas jurídicas de direito privado controladas pelo Poder Público, mas com personalidade jurídica de direito privado (caso do SERPRO, que é empresa pública)[23]. Essa novidade se alinha às proposições doutrinárias mais recentes quanto ao fato de não ser possível admitir que

"as mudanças estruturais se limitem à exteriorização da relação jurídica mantida entre Administração Pública e administrado, devendo ser direcionado um olhar atento e rigoroso ao processo interno de implantação de melhorias por parte do Estado e que gerem adesão por aqueles que são responsáveis por desempenhar diariamente a função pública"[24].

No § 1º do artigo 26, que cuida do compartilhamento de dados pelo Poder Público, foram mantidas as inclusões dos incisos IV e V – alternativos, e não cumulativos[25] –, mas houve veto ao inciso VI, que cuidava dos dados acessíveis publicamente. Por outro lado, foi consolidada a nova redação dada ao artigo 29, pela MP 869, que apenas delineou com maior clareza a possibilidade de que se solicite não apenas às entidades do Poder Público (Administração indireta), mas também a seus órgãos (Administração direta), "informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado".

No artigo 5º, foram realizados pequenos ajustes redacionais aos seguintes incisos: a) inc. VIII, para inserir, em sua parte final, a nomenclatura correta da autoridade nacional (Agência Nacional de Proteção de Dados – ANPD); b) inc. XVIII, com mera conversão da nova redação conferida pela MP 869/2018 (LGL\2018\12628); c) inc. XIX, com o acréscimo, ao final, da expressão "em todo o território nacional", deixando ainda mais claro o escopo de atuação da Agência Nacional de Proteção de Dados.

Ao artigo 7º, que cuida das hipóteses em que é permitido o tratamento de dados pessoais relativos à saúde[26], se consolidou a seguinte redação ao inciso VIII: "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária." A novidade está no advérbio "exclusivamente", inserido para garantir a sintonia da LGPD com o disposto no artigo 1º da Resolução 1.605/2000 e no artigo 1º da Resolução 1.638/2002, ambas do Conselho Federal de Medicina (CFM), que sinalizam a imperiosidade do sigilo de dados dessa estirpe[27].

Em igual sentido, mas em relação aos dados pessoais sensíveis[28], adaptou-se a redação do artigo 11, inciso II, "f", que agora consta com o seguinte texto: "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária."

Incluiu-se ainda o § 4º ao art. 11 da LGPD, de modo a permitir o uso compartilhado ou a comunicação de dados sensíveis entre controladores que extraem proveito econômico de suas atividades unicamente nas hipóteses de portabilidade de dados (mediante prévio consentimento ou autorização) ou de transações financeiras e administrativas resultantes do uso e prestação dos serviços de prestação de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º do mesmo dispositivo, que ressalva a necessidade de haver um benefício ao interesse do titular dos dados.[29]

A portabilidade de dados já está tratada no artigo 18, inciso V, da Lei, mas a reiteração constante do inciso I do § 4º do artigo 11 se mostra imprescindível, na medida em que, "quanto mais difícil for para um indivíduo mover seus dados, maior é o poder de mercado detido pelo fornecedor, o que gera dificuldades e impossibilita o sucesso de novos entrantes"[30]. Da mesma forma, o inciso II do § 4º corrobora a autodeterminação informativa, realçando direitos do titular para a proteção de dados sensíveis seus.

O § 5º, por sua vez, impõe freios à potencial discriminação praticada por operadoras de planos privados de assistência à saúde, resguardando a confiança, sendo pertinente, nesse ponto, a doutrina de Fernando Martins:

"(...) a confiança (a legítima expectativa gerada pelo predisponente) abre hipóteses normativas, ensejando hermenêutica conformadora aos direitos fundamentais a partir das seguintes ponderações: i) a aplicação do princípio da boa-fé objetiva (no manancial das funções interpretativas, integrativas e limitativas de exercício de posição jurídica); ii) cobertura e execução contratual conforme o tráfego despertado, especialmente no que concerne à natureza dos riscos envolvidos; iii)

controle de conteúdo das cláusulas contratuais que transferem riscos ao vulnerável e oneram o contrato; iv) relevo diferenciado aos anos de contribuição do consumidor como grupo de saúde empresarial (relacionamento contratual); v) proteção da relação médico-paciente existente em face da intervenção indevida pelas operadoras de saúde; e vi) exigência do consentimento esclarecido do consumidor frente ao contrato e aos tratamentos como ordem pública procedimental."[31]

Ainda acerca da portabilidade de dados[32], a Lei 13.853 consolidou a redação do inciso V e do § 6º do artigo 18 da LGPD, vinculando tal direito à posterior regulamentação deixada a cargo da autoridade nacional. De fato, o papel da ANPD, no exercício de seu poder regulamentar infralegal, será crucial para a efetivação deste e de outros direitos contidos na lei.

A nova redação do artigo 20, que aborda o tratamento automatizado, foi mantida nos mesmos moldes definidos pela MP 869/2018 (LGL\2018\12628). Igualmente, o artigo 23, inciso III, teve sua redação mantida, com a inserção da conjunção "e" ao seu final – que delimitaria sua cumulação com o inciso IV, acrescentado pela nova lei, não tivesse esse sido vetado[33].

A figura do encarregado também merece breve comentário, pois receberia uma série de importantes ajustes, notadamente quanto ao regime de responsabilidade civil que lhe é aplicável. Sobre esta figura, porém, o veto presidencial[34] ao § 4º do artigo 41 culminou na manutenção da norma precedente.

Com o veto, também foram afastados os três incisos que acompanhariam o acima mencionado § 4º, e que compunham o elenco de matérias a serem regulamentadas pela ANPD: i) os casos em que o operador deveria indicar encarregado; ii) a indicação de um único encarregado, desde que facilitado o seu acesso, por empresas ou entidades de um mesmo grupo econômico; iii) a garantia da autonomia técnica e profissional no exercício do cargo.

Devido à ausência de menção expressa à responsabilidade civil do encarregado de dados – responsável por passar instruções ao controlador e a seus colaboradores quanto à proteção de dados – no artigo 42, nota-se sonora lacuna, uma vez que se trata de figura central para o controle de eventos danosos, na medida em que a exaração de qualquer espécie de comando errôneo, por parte do encarregado, pode vir a causar dano e, para solucionar o caso, impõe-se a leitura do artigo 43, inciso III, que expressamente afasta a responsabilidade civil dos agentes de tratamento (controladores e operadores) quando esta puder ser transferida a terceiro, o que permitiria responsabilizar o encarregado na hipótese descrita, embora, para isso, seja passível de invocação a disciplina jurídica contida noutras fontes normativas, como o Código Civil (LGL\2002\400) e o Código de Defesa do Consumidor.

Finalmente, merece destaque a delimitação das normas concernentes à implementação da Agência Nacional de Proteção de Dados, tema que foi amplamente debatido nas audiências públicas realizadas pelo Congresso Nacional, pois, indubitavelmente, a existência de uma autoridade nacional independente é aspecto fundamental para a efetivação da lei.

Importante estudo realizado na Austrália mostrou que, em todo o mundo, autoridades nacionais realmente fortes existem na grande maioria dos países que já possuem normas de proteção de dados. Foram averiguados 132 países e constatou-se que apenas 10% (dez por cento) não criaram autoridades específicas e 10% (dez por cento) demoraram muito para fazê-lo, e, no majoritário rol de países que criaram agências com perfil adequado, seu caráter independente foi festejado pelo estudo. Inclusive, às autoridades não dotadas de independência foi reservado, pelo autor do estudo, um lugar no "*Hall of Shame*"[35].

Nesse compasso, a redação final da Lei nº 13.853/2019 (LGL\2019\5777) assim tratou do assunto, em seu artigo 55-A:

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

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2

(dois) anos da data da entrada em vigor da estrutura regimental da ANPD.

§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias."

Se o texto original da LGPD, aprovado em agosto de 2018, previa a criação de uma entidade, com natureza autárquica e, portanto, pertencente à Administração Pública indireta no plano federal, a MP 869/2018 (LGL\2018\12628), convertida na Lei 13.853/19 (LGL\2019\5777), andou em sentido diametralmente oposto, criando-a como órgão vinculado à Presidência da República[36]. Agora, na consolidação do texto final da reforma, nota-se o intuito de equacionar a questão, com a criação da ANPD como órgão, mas de natureza transitória, sendo possivelmente transformada em entidade (autarquia) *a posteriori*.

Naturalmente, a inserção do verbo "poderá" no § 1º do artigo 55-A causa algum receio, uma vez que deixa em aberto certo grau de discricionariedade para a efetiva conversão do novo órgão em entidade, embora o § 2º delimite um prazo de até 2 (dois) anos para que esta decisão seja tomada.

Ao mesmo tempo que se clama pela efetivação da proteção de dados para a estabilização das relações sociais travadas na Internet, diversas nuances permanecem nebulosas, mesmo com reformas, ajustes, audiências públicas, alterações e proposições para a adaptação estrutural do Estado em relação a seu aparelhamento voltado ao atendimento de seus deveres de proteção[37].

Espera-se que a consolidação legislativa de tão importante direito fundamental – a proteção de dados pessoais – sacramente uma mudança profunda na forma de realização das atividades de Estado para que se prime pela independência de quem, ao fim e ao cabo, deverá assumir a função de regulamentar, fiscalizar e aplicar sanções.

Constata-se que as mudanças já realizadas na Lei Geral de Proteção de Dados brasileira sinalizam a preocupação do legislador com a confiabilidade de seu texto final, repleto de nuances complexas e que demandarão de todos os agentes de dados profundas adaptações em suas rotinas relacionadas às operações de coleta e tratamento de dados.

Em breves linhas, procurou-se averiguar, pontualmente, as principais modificações realizadas pela Lei 13.853, de 08 de julho de 2019 (LGL\2019\5777), que consolidou o texto anterior, que já havia sido alterado pela Medida Provisória 869, de 27 de dezembro de 2018 (LGL\2018\12628). Anotou-se que, em grande parte, o legislador buscou esclarecer o escopo de aplicação da normativa, particularmente no que diz respeito ao Estado e às suas atividades enquanto agente de dados e, também, enquanto responsável por fiscalizar e sancionar atividades realizadas em desconformidade com os ditames da lei.

A preocupação com dados relacionados à saúde e dados acadêmicos reafirma essa cautela mais ampla com determinadas espécies de dados, ao passo que questões como o tratamento automatizado ainda parecem suscitar dúvidas quanto a seu escopo de proteção.

É inegável que a consolidação do texto que cria a Agência Nacional de Proteção de Dados reforça o papel crucial que tal órgão terá, ao fim do período de *vacatio legis*, para que não se tenha o esvaziamento da norma. Espera-se, ademais, que sua conversão de órgão da Administração direta em entidade (autarquia) da Administração indireta, no plano federal, venha a se concretizar, assegurando-se maior independência em sua atuação.

O Decreto 10.046, de 07 de outubro de 2019, versa sobre a governança e o compartilhamento de dados na administração pública federal, já previsto, de forma programática, no artigo 27 da LGPD. O Decreto assim prevê, no seu artigo 1º:

"Art. 1º Este Decreto estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, com a finalidade de:

I – simplificar a oferta de serviços públicos;

II – orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas

públicas;

III – possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;

IV – promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e

V – aumentar a qualidade e a eficiência das operações internas da administração pública federal."

Sendo certo que o *Big Data* público já é uma realidade, o controle de dados exercido pelo poder público ganha nova dimensão, com a possibilidade de compartilhamento entre órgãos. A criação do "Cadastro Base do Cidadão" (art. 16 e seguintes), por exemplo, bem como o cruzamento de dados extraídos de bases como a Receita Federal do Brasil e do Instituto Nacional do Seguro Social, propiciam a consolidação de uma vigilância de dados estatal.

Posteriormente, a União, com a promulgação do Decreto 10.222, de 5 de fevereiro de 2020 (LGL\2020\1059), aprovou a Estratégia Nacional de Segurança Cibernética, cujo artigo 1º remete ao conforme o disposto no inciso I do art. 6º do Decreto nº 9.637, de 26 de dezembro de 2018 (LGL\2018\12446).[38]

Em que pesem as críticas, é em tempo que o Brasil aprova uma Lei Geral de Proteção de Dados, procurando se adequar aos *standards* de proteção europeus, hoje referência para o mundo especialmente após escândalos como o do Facebook com a empresa Cambridge Analytica, divulgado pela imprensa no ano de 2018. Desenvolvido por um professor da Universidade de Cambridge, Inglaterra, Aleksandr Kogan, o aparentemente inofensivo aplicativo sobre a "vida digital" teve a adesão de 270 mil internautas. Por meio deles, chegando aos respectivos amigos na rede social, o mecanismo capturou informações pessoais de 87 milhões de usuários do Facebook.[39]

Foi tudo repassado para a empresa Cambridge Analytica, que, por meio de sofisticadas ferramentas digitais, identificou pessoas suscetíveis a determinadas mensagens, como contra imigrantes, de teor ultranacionalista etc. Tais pessoas passaram a ser bombardeadas pelas informações *fakes*, e foi assim que votos decisivos terminaram sendo conquistados na Grã-Bretanha para que o projeto do Brexit, a saída da União Europeia, ganhasse o plebiscito de 2016 pela estreita margem de quatro pontos percentuais (de 52% a 48%).[40]

As preferências dos titulares, que foram indevidamente utilizadas, através de uma autorização colhida por meio tortuoso, influenciaram ainda a eleição de Donald Trump, nos Estados Unidos, também em 2016, quando ele perdeu na eleição popular, mas ganhou em distritos-chave que lhe garantiram os votos necessários para se eleger no colégio eleitoral. Curioso salientar que o presidente da empresa à época, Steve Bannon – famoso por administrar um blog de "*alternative right* " (em outras palavras, extrema direita) – acabou coordenando a campanha do então presidente norte-americano.

Tal fato inclusive acarretou a aplicação, no Brasil, de multa de R$ 6,6 milhões, pela Secretaria Nacional do Consumidor do Ministério da Justiça, ao Facebook, devido ao compartilhamento de informações de brasileiros.

Os dados pessoais têm sido utilizados por governos e grandes *players* econômicos para a criação de um *one-way mirror,* possibilitando que tais agentes saibam tudo dos cidadãos, enquanto esses nada sabem dos primeiros. Isso acontece por meio de um monitoramento e vigília constantes sobre cada passo da vida das pessoas, levando a um capitalismo de vigilância, cuja principal consequência é a constituição de uma sociedade também de vigilância.[41]

De fato, a experiência do comércio eletrônico transmite ao consumidor uma sensação de liberdade e de amplo poder de escolha, quando, na verdade, as empresas controlam toda a informação e, não raro, aproveitam a assimetria de informação para explorar o consumidor.[42]

Outra característica marcante da atual sociedade de massa é a oferta pelos prestadores ditos *gratuitos*, normalmente baseada na remuneração indireta, igualmente a atrair a incidência das normas do Código de Defesa do Consumidor. É o caso dos provedores de aplicações de Internet que administram as redes sociais virtuais.

Longe de ser uma realidade restrita a regiões ou a países determinados, as práticas perpassam os costumes e penetram a cultura de cada sociedade, multiplicando em progressão geométrica o número de usuários. Formam-se gigantescos bancos de dados de caráter pessoal a serviço de entidades de caráter privado, cujos interesses econômicos frequentemente se impõem de maneira agressiva.

Deve haver, portanto, um contraponto, através do tratamento de dados pessoais. Mesmo diante de tal controle, há a dificuldade de se individuar tipos de informações acerca dos quais o cidadão estaria disposto a renunciar definitivamente, visto que até mesmo os dados mais inócuos podem, se associados a outros, provocar danos à dignidade do interessado.[43]

A nova situação determinada pelo uso de computadores no tratamento de informações pessoais torna cada vez mais difícil considerar o cidadão como um simples "fornecedor de dados", sem que a ele caiba algum poder de controle, ensina Stefano Rodotà, problema esse que ultrapassa as fronteiras individuais e se dilata na dimensão coletiva.[44]

Observe-se que a informação em si não tem valor significativo, mas sim o que se pode fazer com ela, viabilizando uma série de condutas, como o *marketing* direto, ou a determinação de um perfil do usuário sem que esse saiba, de modo que a obtenção de lucro é inevitável diante da utilização das informações. Outro exemplo é o chamado *Big Data,* ou seja, informações de todo tipo podem ser associadas de tal forma a determinar um conteúdo de relevância à soberania estatal, à dignidade da pessoa humana, por exemplo, prevenir doenças, a pornografia infantil ou atos de terrorismo e racismo.[45]

Destaca-se um fato ocorrido nos Estados Unidos da América, em que, semanas antes de se diagnosticar o vírus H1N1, engenheiros da Google publicaram um artigo no jornal científico *Nature,* explicando como conseguiram prever a epidemia causada pelo vírus. A empresa conseguiu esse resultado através do monitoramento das pesquisas realizadas por seus usuários.

No entanto, o uso dessas informações pode ser nocivo. Por exemplo, se tais informações forem passadas para os laboratórios para aumentarem o preço de determinado medicamento; ou em razão do histórico da navegação do usuário, tais informações forem passadas para a seguradora calcular o risco. Para o Direito Digital a prática denominada *profiling* (ou "perfilamento", como se convencionou denominar em português)[46] possui grande importância, pois reflete uma faceta da utilização dos algoritmos que, empregados nos processos de tratamento de grandes acervos de dados (*Big Data*), propiciam o delineamento do "perfil comportamental" do indivíduo, que passa a ser analisado e objetificado a partir dessas projeções.

Na LGPD, dispositivo bastante tímido, inserido em um único parágrafo do artigo que cuida da anonimização de dados (artigo 12, § 2º), conceitua a referida prática: "Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada."[47]

Essa situação é amplificada em tempos de pandemia, pois se almeja amplo controle populacional a partir da vigilância de dados (*dataveillance*).[48] Com isso, iniciativas de monitoramento passam a ser festejadas e não mais repudiadas e exemplo disso já se notou anos atrás, em 2009, por ocasião da pandemia da *Influenza H1N1*, no Reino Unido[49], onde operadoras de telefonia móvel foram instadas a fornecer dados de geolocalização de seus usuários ao governo britânico.

O mesmo cenário vem se repetindo com a *Covid-19*. Na China, foi lançado um aplicativo que cruza dados da Comissão Nacional de Saúde, do Ministério de Transportes e da Agência de Aviação Civil, a fim de identificar indivíduos que tiveram contato com pessoas infectadas (ou com suspeita de infecção pelo vírus), o que, segundo a justificativa apresentada, possibilita reprimir a exponencial transmissão da *Covid-19*, antes mesmo de se ter certeza se a pessoa fora ou não infectada.[50]

Iniciativas semelhantes também estão sendo vistas no Brasil. No Estado de São Paulo, pioneiro na implementação dessa espécie de medida, uma parceria do governo estadual com as operadoras Vivo, Claro, Oi e TIM passou a alimentar um sistema denominado Simi-SP, sob a seguinte justificativa:

"Com o Simi-SP, o Governo de São Paulo pode consultar informações georreferenciadas de mobilidade urbana em tempo real nos municípios paulistas. Para garantir a privacidade de cada

cidadão, o monitoramento é feito com base em dados coletivos coletados em aglomerados a partir de 30 mil pessoas."[51]

Medidas parecidas também foram noticiadas no Rio de Janeiro.[52]

Após o anúncio das medidas adotadas pelos governos estaduais, a União também se mobilizou, pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), que se uniu às quatro operadoras citadas, incluindo ainda uma quinta (Algar Telecom), para que, a partir das informações de suas torres de transmissão, que podem identificar a movimentação das pessoas, seja realizado o monitoramento de dados de 220 milhões de aparelhos móveis[53], a partir de dados que, segundo informaram "estão uma camada acima dos dados pessoais".[54] Seriam dados anonimizados, portanto.[55]

Num panorama de vigilância líquida e distribuída, em que parece ocorrer uma erosão da esfera de controle de dados pessoais, os respectivos titulares são submetidos a uma condição de hipervulnerabilidade, sobretudo por estarem inseridos numa relação assimétrica que lhes tolhe o poder de autodeterminação. Espera-se que, nesse panorama, a nova legislação contribua para reduzir a flagrante assimetria entre as partes.

3. Os princípios gerais da proteção de dados pessoais

A partir do disposto na Constituição da República e da Lei de Proteção de Dados Pessoais, é possível verificar uma imposição de princípios básicos a que deve obedecer a utilização da informática aplicada ao tratamento de dados, especialmente no tocante aos direitos fundamentais e à ordem constitucional do Estado Social e Democrático de Direito.

Destacam-se, no artigo 6º da LGPD, [56], os seguintes princípios, que atuam como mandamentos do sistema: o princípio da boa-fé (*caput*), o princípio da finalidade (inciso I), o princípio da adequação (inciso II), o princípio da necessidade (inciso III), o princípio do livre acesso (inciso IV), o princípio da qualidade dos dados (inciso V), o princípio da transparência (inciso VI), o princípio da segurança (inciso VII), o princípio da prevenção (inciso VIII), o princípio da não discriminação (inciso IX) e o princípio da responsabilização e da prestação de contas (inciso X).

3.1. Princípio da boa-fé

O art. 6º, *caput,* da LGPD define que as atividades de tratamento de dados pessoais deverão observar a boa-fé. A boa-fé objetiva[57] corresponde a deveres de conduta contratuais, de natureza secundária, lateral, anexa ou instrumental, tais quais os de informação correta, esclarecimento, lealdade e assistência, entre outros[58], encontrando-se consagrada nos arts. 4º, III e 51, IV, da Lei 8.078/90 (LGL\1990\40), que dialogam com as normas gerais dos artigos 113, 187 e 422 do Código Civil (LGL\2002\400).

A boa-fé contratual, que compreende o principal campo de atuação da boa-fé objetiva, corresponde a uma real expectativa legítima por parte do consumidor do produto ou serviço, que deve ter motivos para confiar na contraparte[59].

A boa-fé objetiva, decorrente da concepção da obrigação como processo, implica uma conduta de cooperação, lealdade e expectativas legítimas das partes, em especial o titular, face ao controlador (art. 10, II, LGPD), o que se delineia a partir das circunstâncias concretas em que se deu o consentimento, a finalidade de uso e o tratamento de dados indicado, assim como as informações prévias oferecidas. A tutela da confiança do consumidor abrange tanto a crença nas informações prestadas quanto de que aquele que tenha acesso aos seus dados, por força do consentimento dado, não se comporte de modo contraditório a elas e respeite a vinculação à finalidade de utilização.[60]

A boa-fé, além de prevista como norte das atividades de tratamento de dados pessoais, inclusive no seu uso secundário[61]; além de contemplada no art. 6º, *caput,* é também prevista no artigo 7º, § 3º ("o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização"), bem como constitui parâmetro e critério para a aplicação de sanções administrativas, conforme o artigo 52, § 1º, II, da LGPD.[62]

A boa-fé contratual, que compreende o principal campo de atuação da boa-fé objetiva, corresponde a

uma real expectativa legítima por parte do consumidor do produto ou do serviço, que deve ter motivos para confiar na contraparte[63].

3.2. Princípio da finalidade

Afirma-se que todo procedimento ligado ao sistema de tratamento de dados, automatizado ou não, deve ser realizado sempre e exclusivamente no sentido de atingir os objetivos propostos para o sistema[64]. Por isso, é preciso observar os critérios de proporcionalidade e de adequação entre os meios e os fins, em todas as etapas do processamento das informações, que se concretizam em requisitos de limitação: da coleta e do armazenamento; da conservação, do uso e da comunicação dos dados[65].

A finalidade deve ser conhecida antes de que ocorra a coleta dos dados, especificando-se sobretudo na relação entre os dados colhidos e seu objetivo, além da sua utilização não abusiva e na eliminação ou anonimização dos dados que não mais se tornarem necessários.[66]

O artigo 6º, I, da LGPD define o princípio da finalidade, vinculando-o à "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Com base nesse princípio fundamenta-se a restrição da transferência de dados pessoais a terceiros, além de se poder, através dele, estruturar um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade, fora da qual haveria abusividade. [67]

O art. 7º da LGPD, como visto, define as finalidades legítimas para o tratamento de dados pessoais. [68] Em relação aos dados pessoais sensíveis, tais finalidades são definidas, de modo mais estrito, no artigo 11 da LGPD.[69]

Isso justifica uma limitação da coleta e armazenamento de dados, de modo que tais procedimentos devem sempre se limitar às informações estritamente necessárias à finalidade da operação.[70] Da mesma forma, a qualidade dos dados evidencia a obediência a esse princípio: os dados devem ser completos, exatos, pertinentes e relevantes aos fins propostos[71].

Aquele que pretende obter o consentimento do titular dos dados obriga-se a declinar expressamente as finalidades para as quais pretende utilizar os dados, vinculando-se aos termos desta sua manifestação pré-negocial.

Deve-se ter o cuidado redobrado com relação à coleta e ao armazenamento de informações consideradas "sensíveis", na presunção de que não seriam relevantes ou necessárias aos objetivos de qualquer banco de dados; ou, se o forem, não serão a ponto de dissipar o interesse de cada um no resguardo de sua intimidade ou na prevenção de seu uso com fins discriminatórios[72].

A finalidade compreende ainda a limitação temporal do tratamento de dados, de modo que as informações coletadas e armazenadas não devem permanecer nos bancos de dados por um período de tempo maior do que o essencialmente necessário ao atingimento dos fins propostos[73].O artigo 15 da LGPD prevê as hipóteses do término do tratamento dos dados pessoais.

3.3. Princípio da adequação

A adequação é definida no artigo 6º, II, da LGPD pela "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Esse princípio tem em foco o procedimento empregado para chegar à finalidade pretendida. [74]

Seu objetivo é preservar a vinculação necessária entre a finalidade de utilização dos dados informada ao titular e seu efetivo atendimento na realização concreta do tratamento dos dados. Vincula-se diretamente ao consentimento dado pelo titular para o tratamento dos dados ou às demais finalidades legais admitidas, que deverão ser informadas, lado a lado com a situação de confiança que se cria a partir do estrito atendimento nos termos da informação prévia ao consentimento ou ao uso informado.[75]

3.4. Princípio da necessidade

Trata-se, segundo o artigo 6º, III, da LGPD, da "limitação do tratamento ao mínimo necessário para a

realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

O uso dos dados pessoais, portanto, deve se restringir ao mínimo necessário que atenda aos fins de consentimento do titular e finalidade legítima, observada a adequação entre meios e fins, de maneira pertinente, proporcional e não excessiva.[76]

3.5. Princípio do livre acesso

Conforme a definição legal do artigo 6º, IV, da LGPD, consiste o livre acesso na "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais".

Ligado à publicidade, seu objetivo é resguardar a efetiva participação dos titulares dos dados no seu tratamento[77], expressada na exigência de consentimento e na possibilidade de conhecimento sobre a forma e a extensão em que se desenvolve tal atividade. Abrange inclusive a possibilidade de obter cópia dos registros existentes, bem como corrigir informações incorretas ou imprecisas, podendo inclusive acrescentar dados verdadeiros que possam favorecer seu interesse.[78]

Há ainda referência ao livre acesso no art. 9º da LGPD, em relação às informações sobre o tratamento dos dados pelo titular, devendo essas serem disponibilizadas de maneira clara, adequada e ostensiva acerca de, entre outras características previstas em regulamento, sejam observadas: I – a finalidade específica do tratamento; II – a forma e duração do tratamento, observados os segredos comercial e industrial; III – a identificação do controlador; IV- as informações de contato do controlador; V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI – responsabilidades dos agentes que realizarão o tratamento; e VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

Como bem observa Bruno Miragem, a violação do direito de acesso aos dados pode se caracterizar não só pela simples recusa, mas, na dinâmica atual do mercado de consumo, pela imposição de obstáculos ao acesso, exigindo que o consumidor se reporte a diferentes pessoas ou setores distintos para obter a informação, retardando injustificadamente seu acesso e deixando de facilitar o exercício do direito.[79]

3.6. Princípio da qualidade dos dados

A LGPD, em seu artigo 6º, V, assegura a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento".

3.7. Princípio da transparência

A transparência é definida pelo artigo 6º, VI, da LGPD como a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

Encontra-se referência à transparência sobre o procedimento de tratamento de dados e os sujeitos envolvidos em diversos sistemas jurídicos, inclusive no artigo 39 do RGPD, Regulamento 679/2016 da Comunidade Europeia, em cujos termos "deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados".[80]

De acordo com o princípio da transparência, todo sistema de coleta, registro, tratamento, processamento, transmissão e de banco de dados deve ser do conhecimento público. Segundo José Adércio Leite Sampaio, isso significa que todos – ou pelo menos aqueles cujos dados tenham sido coletados, registrados, tratados, processados, transmitidos ou armazenados em bancos – devam e possam ter ciência do tipo de informação envolvida, bem como da finalidade da operação envolvida, seja através de publicações periódicas de relatórios pelas unidades de processamento, seja pela disponibilização dos dados, de forma *on-line* ou não, em escritórios especializados ou até mesmo em bibliotecas e livrarias[81].

O princípio da transparência se concretiza a partir de algumas exigências a serem feitas ao responsável pela coleta, pelo registro, pelo tratamento, pelo processamento, pela transmissão e pela manutenção de bancos de dados, tais como:

(a) a exigência de que peça autorização prévia para o funcionamento de qualquer sistema com essa finalidade;

(b) a exigência do registro da instalação do sistema;

(c) a exigência de relatórios periódicos das atividades, contendo a existência e a natureza de suas atividades, especificando o tipo de informação armazenada, os procedimentos adotados, as formas de recuperação, o acesso, a retenção e a disponibilização dos dados armazenados, a finalidade do armazenamento, as pessoas envolvidas, os estabelecimentos para os quais regularmente serão transmitidos ou comunicados os dados e o tipo de dado que será comunicado;

(d) a exigência da ciência dos envolvidos; as pessoas cujos dados estejam sendo coletados ou tratados devem ser cientificadas do assunto. O órgão responsável pela coleta, pelo registro, pelo tratamento, pelo processamento, pela transmissão e pela manutenção de bancos de dados deve prestar esclarecimentos à pessoa submetida à coleta de informações com relação ao caráter facultativo ou obrigatório das respostas, as consequências de uma ausência de resposta, os destinatários das informações e a existência do direito de acesso e de retificação.

Há uma preocupação com relação à legítima expectativa do titular dos dados, mas, sobretudo, a determinação do controle do tratamento pelo titular dos dados em relação ao compromisso assumido pelo controlador por ocasião da obtenção dos dados.[82]

A transparência pode ser extraída de alguns dispositivos da LGPD, como o art. 9º, § 1º ("na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca"), o artigo 10, § 2º ("o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse") e o artigo 40 ("a autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência").[83]

Assinale-se que o princípio da transparência não é absoluto. Admitem-se exceções com relação à defesa nacional, à segurança pública, à prevenção do crime, à cobrança de impostos e taxas, a certas autoridades da Receita Federal, a programas sociais ou à saúde pública[84].

Além disso, afirma-se que há uma tendência, embora discutível, de se tornarem menos rígidas as exigências para a instalação de bancos de dados pessoais, se tais dados se referirem a assuntos rotineiros, que não ofereçam riscos aos direitos fundamentais, como aqueles destinados à simples listagem de empregados, de materiais de estoque, de modelos de correspondência e documentos, ou com finalidade puramente doméstica ou de entretenimento[85].

3.8. Princípio da segurança

A segurança é definida pelo artigo 6º, VII, da LGPD como a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Trata-se de um desdobramento da segurança exigida do fornecedor em face da pessoa e do patrimônio do consumidor, cuja violação (CDC (LGL\1990\40), arts. 12 e 14; LGPD, arts. 42 e seguintes) implica a responsabilidade objetiva pelos danos causados, inclusive na hipótese de os dados serem acessados sem autorização ou acidentalmente, o que compreende ainda as hipóteses de destruição, perda, alteração, comunicação ou difusão. [86]

O artigo 44 dispõe que "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes", ao passo que o artigo 46 e seguintes contemplam regras sobre segurança e boas práticas.

3.9. Princípio da prevenção

Dentro do direito a não ser vítima de danos, a prevenção é definida pelo art. 6º, VIII, da LGPD como a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

3.10. Princípio da não discriminação

A não discriminação é conceituada pelo artigo 6º, IX, da LGPD como a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". A grande vantagem propiciada pelo processamento de dados pessoais, no sentido da maior precisão da segmentação e da personalização dos consumidores, não pode servir para prejudicar, restringir ou excluir qualquer consumidor da possibilidade de acesso ao consumo. [87]

O que a lei proíbe, como em relação ao *geopricing* e ao *geoblocking*, condutas ilegítimas que inclusive atentam contra a neutralidade da Internet (art. 9º do Marco Civil), ao precificar a oferta (*geopricing*) ou impedir o acesso dos consumidores a determinados bens e serviços conforme sua localização geográfica (*geoblocking*), não é a discriminação em si, mas aquela contaminada de finalidade ilícita ou abusiva. Na prática, a discriminação, envolvendo não só os preços como a figura do consumidor, não é feita de forma clara e transparente, causando prejuízos passíveis de indenização, sem prejuízo da imposição de obrigações de fazer ou não fazer, tendentes a assegurar a prevenção. Se o algoritmo, por sua própria arquitetura, já é construído de modo a discriminar, é necessária uma transparência e informação em relação aos seus mecanismos, o que afastaria a ilicitude ou abusividade da conduta.

Ilícita seria a discriminação baseada em critérios proibidos pela lei para fins de diferenciação, cabendo uma referência à Constituição da República, que, no seu artigo 3º, IV, proíbe preconceitos de origem, raça, sexo, cor e idade. Da mesma forma, estabelece a Lei Maior que "ninguém será privado de direitos por motivo de crença religiosa ou de convicção filosófica ou política" (art. 5º, VIII, Constituição).[88]

É o caso ainda de discriminação em virtude de critérios que não estejam em acordo com a finalidade para a qual se realize determinada diferenciação, como aquela que envolva dados sensíveis, por exemplo, a recusa de fornecimento de produto ou serviço a qualquer pessoa em razão de sua orientação sexual, credo ou raça, ou ainda cobrança de preços diferenciados para homens e mulheres em casas noturnas.

Em relação a essa última situação, a discussão culminou na Nota Técnica 2/2017/GAB-DPDC/DPDC/SENACON, posteriormente revogada, por meio da qual o Ministério da Justiça e Segurança Pública considerou abusiva a mencionada prática, sujeitando eventuais transgressores às sanções previstas no artigo 56 do Código de Defesa do Consumidor (CDC (LGL\1990\40)) e determinando a fiscalização da atividade pelo Sistema Nacional de Defesa do Consumidor.[89]

A análise sistemática das leis brasileiras sobre proteção do consumidor permite entender que existe uma norma de tratamento igualitário aplicável às relações comerciais consumeristas. Ademais, chega-se à mesma conclusão quando se analisa a normativa pátria referente à proteção da ordem econômica. O artigo 36, § 3º, X, da Lei 12.529/2011 (LGL\2011\4796), veda expressamente a discriminação de "adquirentes ou fornecedores de bens ou serviços por meio da fixação diferenciada de preços, ou de condições operacionais de venda ou prestação de serviços".

O direito à não discriminação dialoga ainda com o princípio da equivalência negocial, contemplado no artigo 6º, II, da Lei 8.078/90 (LGL\1990\40), que, sob outro aspecto, assegura ao consumidor o direito de conhecer o produto que está adquirindo, de acordo com a ideia de plena liberdade de escolha, da igualdade nas contratações e do dever anexo de informar. Assim, a lei proíbe qualquer tipo de discriminação no momento de contratar, sob o pretexto constitucional de que todos são iguais perante a lei, existindo também o dever de o prestador ou fornecedor informar todos sobre os riscos inerentes à prestação ou ao fornecimento.

Entre os instrumentos previstos no artigo 20 da LGPD para impedir o tratamento de dados discriminatório está a previsão do direito do titular dos dados de revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito

ou os aspectos de sua personalidade.[90]

Na Comunidade Europeia, a Diretiva 123/2006, de 12 de dezembro, relativa a serviços no mercado interno, prevê, no seu artigo 20, o direito à não discriminação:

"Artigo 20.

Não discriminação

1. Os Estados-Membros devem assegurar que o destinatário não seja submetido a requisitos discriminatórios em razão da sua nacionalidade ou do seu lugar de residência.

2. Os Estados-Membros devem assegurar que as condições gerais de acesso a um serviço que são postas à disposição do grande público pelo prestador não incluam condições discriminatórias baseadas na nacionalidade ou no lugar de residência do destinatário, sem que tal afecte a possibilidade de se preverem diferenças no que diz respeito às condições de acesso e que sejam directamente justificadas por critérios objectivos."

3.11. Princípio da responsabilização e prestação de contas

Tal princípio, na forma do art. 6º, X, da LGPD, encontra seu significado na exigência de comprovação, "pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

A responsabilização e prestação de contas terão eficácia sobretudo na esfera coletiva, sempre que houver interesse difuso, direito coletivo ou direito individual homogêneo, merecedor de proteção diferenciada, em dispositivo que dialoga com o artigo 6º, VI e VII, do Código de Defesa do Consumidor.

Por meio de uma interpretação da Lei da Ação Civil Pública e do Código de Defesa do Consumidor, que trazem os vetores básicos da tutela coletiva brasileira, juntamente com o art. 64 da LGPD, poderá ser proposta ação civil pública não somente para o devido ressarcimento dos danos causados, mas para o emprego da tutela inibitória coletiva, inclusive com medidas de urgência.[91]

Tal conclusão é extraída da literalidade do artigo 22 da LGPD, em cujos termos "a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva".

O artigo 42 da LGPD, no mesmo sentido, contempla a responsabilidade do controlador e do operador que, em razão do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais.

Como decorrência de tal imperativo, a LGPD, no seu artigo 50, previu a obrigatoriedade de programas de *compliance*, em relação aos agentes de tratamento de dados, em especial os controladores e operadores, com a adoção de um programa de governança que atenda a requisitos como as condições de organização, o regime de funcionamento, os procedimentos, inclusive reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

4. Conclusões

Num panorama de vigilância líquida e distribuída, em que parece ocorrer uma erosão da esfera de controle de dados pessoais, os respectivos titulares são submetidos a uma condição de hipervulnerabilidade, sobretudo por estarem inseridos numa relação assimétrica que lhes tolhe o poder de autodeterminação. Espera-se que, nesse panorama, a Lei Geral de Proteção de Dados Pessoais, Lei 13.709/2018 (LGL\2018\7222), contribua para reduzir a flagrante assimetria entre as partes.

A LGPD, em seu artigo 42, *caput,* adota um regime de responsabilidade civil objetiva dos

controladores ou operadores que, em razão do exercício ou atividade de tratamento de dados pessoais, causarem a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais. Tal dispositivo inclusive revoga o art. 19 do Marco Civil da Internet, caso o provedor de aplicações de Internet funcione igualmente como controlador ou operador em relação aos dados pessoais dos usuários

5. Bibliografia

AMARAL, Bruno do. Coronavírus: TIM e Prefeitura do Rio assinam acordo para coletar dados de deslocamento. *Teletime*, 23 mar. 2020. Disponível em: [https://teletime.com.br/23/03/2020/coronavirus-tim-e-prefeitura-do-rio-assinam-acordo-para-coletar-dados-de-desloca Acesso em: 17.04.2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* os limites do consentimento. Rio de Janeiro: Forense, 2019.

CARNEIRO, Isabelle da Nóbrega Rito; SILVA, Luiza Caldeira Leite; TABACH, Danielle. Tratamento de dados pessoais. In: FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coord.). *Comentários à Lei Geral de Proteção de Dados*: Lei 13.709/2018 (LGL\2018\7222). São Paulo: Ed. RT, 2019.

CLARKE, Roger A. Information technology and dataveillance. *Communications of the ACM*, Nova Iorque, v. 31, n. 5, p. 498-512, maio 1988.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada.* São Paulo: Ed. RT, 2018.

COUTO E SILVA, Clóvis. *A obrigação como processo.* São Paulo: José Bushatsky Editor, 1976.

CRAVO, Daniela Copetti. *Direito à portabilidade de dados*: interface entre defesa da concorrência, do consumidor e proteção de dados. Rio de Janeiro: Lumen Juris, 2018.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis; MALGIERI, Gianclaudio; BESLAY, Laurent; SANCHEZ, Ignacio. The right to data portability in the GDPR: towards user-centric interoperability of digital services. *Computer Law & Security Review,* Reino Unido, v. 34, n. 2, p. 193-203, abr. 2018.

DE LUCCA, Newton; MACIEL, Renata Mota. A Lei 13.709, de 14 de agosto de 2018 (LGL\2018\7222): a disciplina normativa que faltava. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de; MACIEL, Renata Mota (Coord.). *Direito & Internet IV:* sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

DE LUCCA, Newton; LIMA, Cíntia Rosa Pereira de. A Autoridade Nacional de Proteção de Dados Pessoais(ANPD) e Conselho Nacional de Proteção de Dados Pessoais e de Privacidade. In: LIMA, Cíntia Rosa Pereira de. *Comentários à Lei Geral de Proteção de Dados.* São Paulo: Almedina, 2020.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital:* direito privado e Internet. 2. ed. Indaiatuba: Foco, 2019.

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

DU BOIS, François. Social purposes, fundamental rights and the judicial development of private law. In: NOLAN, Donal; ROBERTSON, Andrew (Ed.). *Rights and private law.* Oxford: Hart Publishing, 2012.

DUKAKIS, Ali. China rolls out software surveillance for the COVID-19 pandemic, alarming human rights advocates. *ABC News*, 14 abr. 2020. Disponível em: [https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=7013135 Acesso em: 17.04.2020.

EDITORIAL. Multa ao Facebook é parte de caso mundial de manipulação de eleitores. *Jornal O Globo.* Opinião do Globo. Rio de Janeiro, 02 jan. 2020. Disponível em: [https://oglobo.globo.com/opiniao/multa-ao-facebook-parte-de-caso-mundial-de-manipulacao-de-eleitores-1-24166743

EZRACHI, Ariel; STUCKE, Maurice. *Virtual Competition: the promise and perils of algorithm-driven economy*. Cambridge: Harvard University Press, 2016.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.* São Paulo: Ed. RT, 2019.

GONÇALVES, Vilmar Luiz Graça. Direito administrativo e avanços tecnológicos: desafios e conquistas. In: BECKER, Daniel; FERRARI, Isabela (Coord.). *Regulação 4.0:* novas tecnologias sob a perspectiva regulatória. São Paulo: Ed. RT, 2019

GREENLEAF, Graham. Global Data Privacy 2019: DPAs, PEAs, and their Networks. *University of New South Wales Law Research Series,* Sydney, v. 158, Research Paper n. 19-68, p. 1-7, ago. 2019.

HEUSI, Tálita Rodrigues. Perfil criminal como prova pericial no Brasil. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, Itajaí, v. 5, n. 3, p. 232-250, 2016.

LIMA, Cíntia Rosa Pereira de. Direito ao esquecimento e Internet: o fundamento legal no direito comunitário europeu, no direito italiano e no direito brasileiro. *Doutrinas Essenciais de Direito Constitucional. São Paulo: Ed. RT,* 2015. v. 8.

MAGENTA, Matheus. Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia. *BBC News Brasil*, 3 abr. 2020. Disponível em: [www.bbc.com/portuguese/brasil-52154128]. Acesso em: 17.04.2020.

MARTINS, Fernando Rodrigues. A saúde suplementar como sistema jurídico hipercomplexo e a proteção da confiança. *Revista de Direito do Consumidor*, São Paulo, v. 120, n. 4, p. 77-101, nov.-dez. 2018.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. Nota dos coordenadores. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. *Direito digital:* direito privado e internet. 2. ed. Foco: Indaiatuba, 2019.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz. A pandemia da Covid-19, o "profiling" e a Lei Geral de Proteção de Dados. Disponível em: [www.migalhas.com.br/depeso/325618/a-pandemia-da-covid-19-o-profiling-e-a-lei-geral-de-protecao-de-dados]. Acesso em: 02.05.2020.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018 (LGL\2018\7222)) e o direito do consumidor. *Revista dos Tribunais*, São Paulo, v. 1009, p. 173-222, nov. 2019.

MORAES, Maria Celina Bodin de. O princípio da dignidade humana. In: MORAES, Maria Celina Bodin. *Princípios do direito civil contemporâneo.* Rio de Janeiro: Renovar, 2006.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18 (LGL\2018\7222)). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set.-dez. 2018.

NORONHA, Fernando. *O direito dos contratos e seus princípios fundamentais (autonomia privada, boa-fé e justiça contratual)*. São Paulo: Saraiva, 1994.

PFEIFFER, Roberto Augusto Castellanos. ANPD em busca de sua autonomia: é preciso aperfeiçoar a MP 869/2018 (LGL\2018\12628). *Jota*. 1º de maio de 2019. Disponível em: [www.conjur.com.br/2019-mai-01/garantias-consumo-anpd-busca-autonomia-preciso-aperfeicoar-mp]. Acesso em: 03.08.2019.

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

ROMANI, Bruno. Uso de dados de localização no combate à covid-19 pode ameaçar privacidade. *O Estado de S. Paulo*, 12 abr. 2020. Disponível em: [https://link.estadao.com.br/noticias/cultura-digital,uso-de-dados-de-localizacao-no-combate-a-covid-19-pode-ameacar

Acesso em: 17.04.2020.

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: [http:civilistica.com/-o-consentimento-informado-e-a-protecao]. Acesso em: 19.07.2019.

SARLET, Ingo Wolfgang; KEINERT, Tania Margarete Mezzomo. O direito fundamental à privacidade e as informações em saúde: alguns desafios. In: KEINERT, Tânia Margarete Mezzomo et al (Org.). *Proteção à privacidade e acesso às informações em saúde*: tecnologias, direitos e ética. São Paulo: Instituto da Saúde, 2015.

SILVA, Agathe S. da. Cláusula geral de boa-fé nos contratos de consumo. *Revista de Direito do Consumidor.* São Paulo, v. 17, p. 146-161, jan.-mar. 1996.

SILVA, Jorge Pereira da. *Deveres do Estado de protecção de direitos fundamentais*: fundamentação e estrutura das relações jusfundamentais triangulares. 3. ed. Lisboa: Universidade Católica Editora, 2015.

SOUSA, Rabindranath Capelo de. *O direito geral de personalidade.* Coimbra: Coimbra Editora, 1995.

TAMÒ-LARRIEUX, Aurelia. *Designing for privacy and its legal framework.:* data protection by design and default for the Internet of Things. Basileia: Springer, 2018.

TILSTON, Natasha L.; EAMES, Ken T.D.; PAOLOTTI, Daniela et al. Internet-based surveillance of Influenza-like-illness in the UK during the 2009 H1N1 influenza pandemic. *BMC Public Health*, Londres, v. 10, p. 650-659, 2010.

ZANATTA, Rafael A. F.; SOUZA, Michel R. O. A tutela coletiva em proteção de dados pessoais: tendências e desafios. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de; MACIEL, Renata Mota. *Direito & Internet IV:* sistema de proteção de dados pessoais. São Paulo: Quarter Latin, 2019.

---

1 .“Nesse sentido, há consenso em torno da ideia de ser a privacidade um princípio fundamental na moderna legislação sobre os Direitos Humanos, dado que é protegida em nível internacional por meio de pelo menos três instrumentos essenciais – também para o caso brasileiro, designadamente, a Declaração Universal dos Direitos Humanos , o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP) e a Convenção Americana de Direitos Humanos (Pacto de São José da Costa Rica), sem prejuízo de outros documentos, da convenção Europeia de Direitos do Homem, e por último, tendo em conta sua relevância, da Carta Europeia de Direitos Fundamentais.” (SARLET, Ingo Wolfgang; KEINERT, Tania Margarete Mezzomo. O direito fundamental à privacidade e as informações em saúde: alguns desafios. *In*: KEINERT, Tânia Margarete Mezzomo et al (Org.). *Proteção à privacidade e acesso às informações em saúde*: tecnologias, direitos e ética. São Paulo: Instituto da Saúde, 2015. p. 118).

2 .Segundo Maria Celina Bodin de Moraes, “O princípio constitucional visa garantir o respeito e a proteção da dignidade humana não apenas no sentido de assegurar um tratamento humano e não degradante, e tampouco conduz ao mero oferecimento de garantias à integridade física do ser humano. Dado o caráter normativo dos princípios constitucionais, princípios que contêm os valores ético-jurídicos fornecidos pela democracia, isto vem a significar a completa transformação do direito civil, de um direito que não mais encontra nos valores individualistas de outrora o seu fundamento axiológico”. (MORAES, Maria Celina Bodin de. O princípio da dignidade humana. In: MORAES, Maria Celina Bodin. *Princípios do direito civil contemporâneo.* Rio de Janeiro: Renovar, 2006. p. 15). A autora decompõe a dignidade humana nos princípios jurídicos da igualdade, da integridade física e

moral – psicofísica –, da liberdade e da solidariedade.

3 .“O modelo jurídico adotado por diversos países para a proteção dos dados pessoais consiste em uma proteção constitucional, por meio da garantia de um direito fundamental, e na concretização desse direito, por meio de um regime legal de proteção de dados, na forma de uma lei geral sobre o tema.”

4 .SOUSA, Rabindranath Capelo de. *O direito geral de personalidade.* Coimbra: Coimbra Editora, 1995, p. 356-357.

5 .SOUSA, Rabindranath Capelo de, op. cit., p. 317.

6 .BIONI, Bruno Ricardo. *Proteção de dados pessoais:* os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 64-65.

7 .BIONI, Bruno Ricardo, op. cit., p. 65.

8 .BIONI, Bruno Ricardo, op. cit., p. 66.

9 .O art. 21 do Código Civil (LGL\2002\400) preconiza a inviolabilidade da “vida privada da pessoa natural”.

10 .*Art. 8º*. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

11 .RODOTÀ, Stefano. *A vida na sociedade da vigilância.* Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 17. A Carta de Direitos Fundamentais da União Europeia, em 2000, reconheceu a proteção de dados como um direito autônomo. Esse pode ser considerado o último ponto de uma longa evolução, separando a privacidade da proteção de dados.

12 .SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*, Rio de Janeiro, ano 8, n. 1, 2019. Disponível em: [http:civilistica.com/-o-consentimento-informado-e-a-protecao]. Acesso em: 19.07.2019.

13 .RODOTÁ, Stefano. *A vida na sociedade da vigilância*, op. cit., p. 19.

14 .MORAES, Maria Celina Bodin de, op. cit., p. 17. Para a autora, “o atual ordenamento jurídico, em vigor desde a promulgação da Constituição Federal de 5 de outubro de 1988, garante tutela especial e privilegiada a toda e qualquer pessoa humana, em suas relações extrapatrimoniais, ao estabelecer como princípio fundamental, ao lado da soberania e cidadania, a dignidade humana. Como regra geral daí decorrente, pode-se dizer que, em todas as relações privadas nas quais venha a ocorrer um conflito entre uma situação jurídica existencial e uma situação jurídica patrimonial, a primeira deverá prevalecer, obedecidos, desta forma, os princípios constitucionais que estabelecem a dignidade da pessoa humana como o valor cardeal do sistema” (op. cit., p. 53).

15 .Acerca da vigência da LGPD, aplica-se o respectivo artigo 65:". Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019 (LGL\2019\5777))

I – dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020 (LGL\2020\7511))

~~II – 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela~~ Lei nº 13.853, de 2019 (LGL\2019\5777)~~)~~

~~II – em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela~~ Medida Provisória nº 959, de 2020 (LGL\2020\5332)~~)~~ (Convertida na Lei nº 14.058, de 2020 (LGL\2020\12507))

II – 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos."

16 .A competência da Autoridade Nacional de Proteção de Dados é disciplinada no Artigo 55-J: "Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

I – zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

II – zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

III – elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

IV – fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

V – apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

VI – promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

VII – promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

VIII – estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

IX – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

X – dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XI – solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XII – elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XIII – editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XIV – ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XV – arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XVI – realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XVII – celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942 (LGL\1942\3); (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XVIII – editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XIX – garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (LGL\2003\582) (Estatuto do Idoso); (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XX – deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XXI – comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XXII – comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XXIII – articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

XXIV – implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019 (LGL\2019\5777))

17 .Merece destaque o artigo 8º da Lei Complementar 866/19, que altera a Lei 12.414/2011 (LGL\2011\1883), cujo artigo 8º, parágrafo único, passa a ter a seguinte redação: “É vedado às fontes estabelecer políticas ou realizar operações que impeçam, limitem ou dificultem a transmissão a banco de dados de informações de cadastrados”.

18 .“Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve

violação à legislação de proteção de dados; ou

III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."

19 .PASQUALE, Frank. *The black box society:* the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 9.

20 .DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital:* direito privado e internet. 2. ed. Indaiatuba: Foco, 2019. p. 52. Destaca o autor: "Assim, e ainda ao elencar dentre seus fundamentos, em seu artigo 2º, outros elementos intrinsecamente ligados à tutela da pessoa e de seus direitos fundamentais, tais quais a autodeterminação informativa, as liberdades de expressão, informação, comunicação e de opinião, a dignidade e o exercício da cidadania, a LGPD estabelece de maneira sólida sua fundamentação nos direitos fundamentais e na proteção da pessoa, o que se verifica igualmente em diversas opções na implementação dos seus mecanismos de tutela (...)."

21 .DU BOIS, François. Social purposes, fundamental rights and the judicial development of private law. In: NOLAN, Donal; ROBERTSON, Andrew (Eds.). *Rights and private law.* Oxford: Hart Publishing, 2012. p. 113. Comenta o autor: "*As a powerful tool for mediating between the common good and the pursuit of individual aims, fundamental rights can assist private law reasoning in this further function. In this regard, they provide a more systematic, transparent and coherent articulation of the concerns that have long bubbled to the surface in the guise of 'public policy' and its cognates, such as 'good faith'. Concepts such as these attest to the role that private law plays in constructing social practices and institutions*."

22 ."Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I – a operação de tratamento seja realizada no território nacional;

II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019 (LGL\2019\5777))

III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional."

23 .No relatório final da lei, optou-se pela referida redação ao § 4º, que havia sido revogado pela MP 869, pelos seguintes motivos (página 58 do documento): "Entendemos que o tratamento da totalidade de bancos de dados de segurança e defesa por empresa privada, aliada ao fato de que essas autoridades não precisem informar a Autoridade quando assim os delegarem, enfraquecem as medidas protetivas da sociedade contra eventuais arbitrariedades e vazamentos de dados sobre tão importante categoria. Ademais, em se tratando de questões de defesa nacional e as conhecidas *back doors* de fabricantes e provedores de aplicações e de bancos de dados que se utilizam de tecnologia estrangeira, há sempre a possibilidade de acesso em nível internacional desses dados. Entretanto, a discussão em Audiência Pública indicou a realidade e a racionalidade de bancos de dados e sistemas de segurança da área de segurança e de investigação serem operados por empresas públicas, tais como o Serpro. Assim, entendemos a necessidade da transferência de dados para tratamento por parte de empresas públicas." (BRASIL. Câmara dos Deputados. *Parecer nº 1/2019 da Comissão Mista de votação da* MP 869/2018 (LGL\2018\12628). Disponível em: [www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=9EC610DD6ADD2D1AD386EA90CAB11DF6.pr
Acesso em: 31.08.2019.

24 .GONÇALVES, Vilmar Luiz Graça. Direito administrativo e avanços tecnológicos: desafios e conquistas. In: BECKER, Daniel; FERRARI, Isabela (Coord.). *Regulação 4.0:* novas tecnologias sob a perspectiva regulatória. São Paulo: Ed. RT, 2019. p. 53.

25 .Eis os incisos: “IV – quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou V – na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.”

26 .CARNEIRO, Isabelle da Nóbrega Rito; SILVA, Luiza Caldeira Leite; TABACH, Danielle. Tratamento de dados pessoais. *In:* FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coord.). *Comentários à Lei Geral de Proteção de Dados*: Lei 13.709/2018 (LGL\2018\7222). São Paulo: Ed. RT, 2019. p. 73. Anotam: “A Lei Federal 8.080/1990 (LGL\1990\41), que regulamenta o direito à saúde, inclui o direito à informação do cidadão e o dever do Estado de fundamentar suas políticas e ações em informações sanitárias e evidências científicas, legitimando a coleta e o uso de informações pessoais. A ideia é que os dados tratados em âmbito da saúde sirvam para garantir a qualidade de vida da sociedade e a redução de riscos ao adoecimento.”

27 .O primeiro dispositivo conceitua o prontuário médico como o “documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo”, ao passo que o segundo dispositivo preconiza que “o médico não pode, sem o consentimento do paciente, revelar o conteúdo do prontuário ou ficha médica.”

28 .Sobre os dados pessoais sensíveis, confira-se: MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18 (LGL\2018\7222)). *Revista de Direitos e Garantias Fundamentais,* Vitória, v. 19, n. 3, p. 159-180, set.-dez. 2018.

29 .“Art. 11. [...] § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I – a portabilidade de dados quando solicitada pelo titular; ou

II – as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo”.

30 .CRAVO, Daniela Copetti. *Direito à portabilidade de dados*: interface entre defesa da concorrência, do consumidor e proteção de dados. Rio de Janeiro: Lumen Juris, 2018. p. 63.

31 .MARTINS, Fernando Rodrigues. A saúde suplementar como sistema jurídico hipercomplexo e a proteção da confiança. *Revista de Direito do Consumidor*, São Paulo, v. 120, n. 4, nov.-dez. 2018. p. 88.

32 .DE HERT, Paul; PAPAKONSTANTINOU, Vagelis; MALGIERI, Gianclaudio; BESLAY, Laurent; SANCHEZ, Ignacio. The right to data portability in the GDPR: towards user-centric interoperability of digital services. *Computer Law & Security Review*, Reino Unido, v. 34, n. 2, abr. 2018, p. 194. Comentam os autores: “The right to data portability is one of the most important novelties within the EU General Data Protection Regulation, both in terms of warranting control rights to data subjects and in terms of being found at the intersection between data protection and other fields of law (competition law, intellectual property, consumer protection, etc.). It constitutes, thus, a valuable case of development and diffusion of effective user-centric privacy enhancing technologies and a first tool to allow individuals to enjoy the immaterial wealth of their personal data in the data economy. Indeed, a free portability of personal data from one controller to another can be a strong tool for data subjects

in order to foster competition of digital services and interoperability of platforms and in order to enhance controllership of individuals on their own data."

33 .A redação do inciso IV previa o seguinte: "IV – sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, no âmbito da Lei 12.527, de 18 de novembro de 2011 (LGL\2011\4603), vedado seu compartilhamento na esfera do poder público e com pessoas jurídicas de direito privado." O veto, entretanto, teve a motivação a seguir: "A propositura legislativa, ao vedar o compartilhamento de dados pessoas no âmbito do Poder Público e com pessoas jurídicas de direto privado, gera insegurança jurídica, tendo em vista que o compartilhamento de informações relacionadas à pessoa natural identificada ou identificável, que não deve ser confundido com a quebra do sigilo ou com o acesso público, é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas. Sob este prisma, e a título de exemplos, tem-se o caso do banco de dados da Previdência Social e do Cadastro Nacional de Informações Sociais, cujas informações são utilizadas para o reconhecimento do direito de seus beneficiários e alimentados a partir do compartilhamento de diversas bases de dados administrados por outros órgãos públicos, bem como algumas atividades afetas ao poder de polícia administrativa que poderiam ser inviabilizadas no âmbito do Sistema Financeiro Nacional."

34 .Com efeito, foram essas as razões do veto: "A propositura legislativa, ao dispor que o encarregado seja detentor de conhecimento jurídico regulatório, contraria o interesse público, na medida em que se constitui em uma exigência com rigor excessivo que se reflete na interferência desnecessária por parte do Estado na discricionariedade para a seleção dos quadros do setor produtivo, bem como ofende direito fundamental, previsto no art. 5º, XIII da Constituição da República, por restringir o livre exercício profissional a ponto de atingir seu núcleo essencial."

35 .GREENLEAF, Graham. Global Data Privacy 2019: DPAs, PEAs, and their Networks. *University of New South Wales Law Research Series,* Sydney, v. 158, Research Paper n. 19-68, p. 1-7, ago. 2019.

36 .PFEIFFER, Roberto Augusto Castellanos. ANPD em busca de sua autonomia: é preciso aperfeiçoar a MP 869/2018 (LGL\2018\12628). *Jota*. 1º de maio de 2019. Disponível em: [www.conjur.com.br/2019-mai-01/garantias-consumo-anpd-busca-autonomia-preciso-aperfeicoar-mp]. Acesso em: 03.08.2019.

37 .SILVA, Jorge Pereira da. *Deveres do Estado de protecção de direitos fundamentais*: fundamentação e estrutura das relações jusfundamentais triangulares. 3. ed. Lisboa: Universidade Católica Editora, 2015. p. 585.

38 .Segue um trecho da introdução ao Anexo do Decreto, sobre a estratégia nacional de segurança cibernérica: "A revolução digital está transformando profundamente nossa sociedade. Nas últimas duas décadas, bilhões de pessoas se beneficiaram do crescimento exponencial do acesso à internet, da rápida adoção dos recursos de tecnologia da informação e comunicação, e das oportunidades econômicas e sociais oriundas do ambiente digital.

Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade.

Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais. Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão.

Em nível superior aos debates sobre a segurança no espaço cibernético está a Segurança da

Informação, área sistêmica, e diretamente relacionada à proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização. Desse modo, segundo o art. 2º do Decreto nº 9.637, de 2018 (LGL\2018\12446), a Segurança da Informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade.

Entende-se que os recursos tecnológicos empregados na segurança sistêmica devem apoiar políticas que garantam os princípios fundamentais da autenticidade e da integridade dos dados, e prover mecanismos para proteção da legitimidade contra sua alteração ou eliminação não autorizada. Do mesmo modo, as informações coletadas, processadas e armazenadas na infraestrutura de tecnologia da informação e comunicação devem ser acessíveis apenas a pessoas, a processos ou a entidades autorizadas, a fim de garantir a confidencialidade das informações. Adicionalmente, os recursos de tecnologia da informação e comunicação devem prover disponibilidade permanente e apoiar de forma contínua todos os acessos autorizados". (Disponível em: [www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm]. Acesso em: 06.02.2020).

39 .MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. Nota dos coordenadores. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. *Direito digital:* direito privado e internet. 2. ed. Foco: Indaiatuba, 2019. p. XXX.

40 .EDITORIAL. Multa ao Facebook é parte de caso mundial de manipulação de eleitores. *Jornal O Globo.* Opinião do Globo. Rio de Janeiro, 02 jan. 2020, p. 2.

41 .FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.* São Paulo: Ed. RT, 2019. p. 27.

42 .EZRACHI, Ariel; STUCKE, Maurice. *Virtual competition: the promise and perils of algorithm-driven economy*. Cambridge: Harvard University Press, 2016. p. 4.

43 .RODOTÀ, Stefano. *A vida na sociedade da vigilância*, cit., p. 36-37: "a obrigação de fornecer dados não pode ser simplesmente considerada como a contrapartida dos benefícios sociais que, direta ou indiretamente, o cidadão pode chegar a aproveitar. As informações coletadas não somente tornam as organizações públicas e privadas capazes de planejar e executar os seus programas, mas permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes: consequentemente, os cidadãos têm o direito de pretender exercer um controle direto sobre aqueles sujeitos aos quais as informações fornecidas atribuirão um crescente *plus-poder*".

44 .Idem.

45 .LIMA, Cíntia Rosa Pereira de. Direito ao esquecimento e INTERNET: o fundamento legal no direito comunitário europeu, no direito italiano e no direito brasileiro. *Doutrinas essenciais de direito constitucional. São* Paulo: Ed. RT, 2015. v. 8. p. 512.

46 .A tradução do termo é colhida das Ciências Criminais, como explica Tálita Heusi: "O perfilamento criminal (*criminal profiling*, em inglês), também tem sido denominado de: perfilagem criminal, perfilamento comportamental, perfilhamento de cena de crime, perfilamento da personalidade criminosa, perfilamento do ofensor, perfilamento psicológico, análise investigativa criminal e psicologia investigativa. Por conta da variedade de métodos e do nível de educação dos profissionais que trabalham nessa área, existe uma grande falta de uniformidade em relação às aplicações e definições desses termos. Consequentemente, os termos são usados inconsistentemente e

indistintamente." (HEUSI, Tálita Rodrigues. Perfil criminal como prova pericial no Brasil. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, Itajaí, v. 5, n. 3, 2016, p. 237).

47 .Acerca do tema, confira-se MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz. A pandemia da Covid-19, o "profiling" e a Lei Geral de Proteção de Dados. Disponível em: [www.migalhas.com.br/depeso/325618/a-pandemia-da-covid-19-o-profiling-e-a-lei-geral-de-protecao-de-dados]. Acesso em: 02.05.2020.

48 .Trata-se de um acrônimo para "*data surveillance*" (vigilância de dados), a indicar uma nova espécie ou técnica de vigilância em razão do surgimento de novos métodos de monitoramento, como a vigilância de dados pessoais e a vigilância de dados em massa, que exigem salvaguardas mais eficazes e uma estrutura política formal. Sobre o tema, confira-se CLARKE, Roger A. *Information technology and dataveillance*. *Communications of the ACM*, Nova Iorque, v. 31, n. 5, p. 498-512, maio 1988.

49 .TILSTON, Natasha L.; EAMES, Ken T.D.; PAOLOTTI, Daniela et al. Internet-based surveillance of Influenza-like-illness in the UK during the 2009 H1N1 influenza pandemic. *BMC Public Health*, Londres, v. 10, p. 650-659, 2010.

50 .DUKAKIS, Ali. China rolls out software surveillance for the COVID-19 pandemic, alarming human rights advocates. *ABC News*, 14 abr. 2020. Disponível em: [https://abcnews.go.com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=7013135 Acesso em: 17.04.2020.

51 .Para mais detalhes: [www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra- Acesso em: 17.04.2020.

52 .AMARAL, Bruno do. Coronavírus: TIM e Prefeitura do Rio assinam acordo para coletar dados de deslocamento. *Teletime*, 23 mar. 2020. Disponível em: [https://teletime.com.br/23/03/2020/coronavirus-tim-e-prefeitura-do-rio-assinam-acordo-para-coletar-dados-de-desloca Acesso em: 17.04.2020.

53 .MAGENTA, Matheus. Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia. *BBC News Brasil*, 3 abr. 2020. Disponível em: [www.bbc.com/portuguese/brasil-52154128]. Acesso em: 17.04.2020.

54 .ROMANI, Bruno. Uso de dados de localização no combate à covid-19 pode ameaçar privacidade. *O Estado de S. Paulo*, 12 abr. 2020. Disponível em: [https://link.estadao.com.br/noticias/cultura-digital,uso-de-dados-de-localizacao-no-combate-a-covid-19-pode-ameacar Acesso em: 17.04.2020.

55 .Define dados anonimizados a LGPD: "Art. 5º (...) III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento."

56 .SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998; DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

57 .Devendo ser extremada em face da boa-fé subjetiva, a qual se refere a um estado interior ou psicológico relativo ao conhecimento, desconhecimento, intenção ou falta de intenção de alguém, a partir de uma situação de aparência que permita ao titular ter expectativas que acredita legítimas, como se verifica em vários preceitos do Código Civil (LGL\2002\400) Brasileiro, tais quais, entre outros, os arts. 1.561 e parágrafos (efeitos do casamento putativo), 1.201, 1.219 e 1.220 (posse de boa-fé), 309 (pagamento a credor putativo), 286 (cessionário de boa-fé) e 896 (portador de boa-fé de título ao portador). Cf. SILVA, Agathe S. Cláusula geral de boa-fé nos contratos de consumo. *Revista de Direito do Consumidor.* São Paulo, v. 17, jan.-mar. 1996. p. 154.

58 .COUTO E SILVA, Clóvis. *A obrigação como processo.* São Paulo: José Bushatsky Editor, 1976. p. 35.

59 .NORONHA, Fernando. *O direito dos contratos e seus princípios fundamentais (autonomia privada, boa-fé e justiça contratual)*. São Paulo: Saraiva, 1994. p. 132 e ss.

60 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018 (LGL\2018\7222)) e o direito do consumidor. *Revista dos Tribunais*, São Paulo, v. 1009, p. 173-222, nov. 2019.

61 .TAMÒ-LARRIEUX, Aurelia. *Designing for privacy and its legal framework.* Data protection by design and default for the Internet of Things. Basileia: Springer, 2018. p. 88 (*e-book*).

62 .DE LUCCA, Newton; MACIEL, Renata Mota. A Lei 13.807, de 14 de agosto de 2018: a disciplina normativa que faltava. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de; MACIEL, Renata Mota (Coord.) *Direito & Internet IV:* sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 46.

63 .NORONHA, Fernando. *O direito dos contratos e seus princípios fundamentais (autonomia privada, boa-fé e justiça contratual)*. São Paulo: Saraiva, 1994. p. 132 e ss.

64 .SAMPAIO, José Adércio Leite, op. cit., p. 513.

65 .SAMPAIO, José Adércio Leite., op. cit., p. 513.

66 .RODOTÁ, Stefano. *A vida na sociedade da vigilância,* op. cit., p. 59.

67 .MIRAGEM, Bruno, A Lei Geral de Proteção de Dados, op. cit., p. 6

68 .“Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de consentimento pelo titular;

II – para o cumprimento de obrigação legal ou regulatória pelo controlador;

III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (LGL\1996\72) (Lei de Arbitragem);

VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019 (LGL\2019\5777))

IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

69 .Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

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

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (LGL\1996\72) (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019 (LGL\2019\5777))

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

70 .TAMÒ-LARRIEUX, Aurelia, op. cit., p. 90.

71 .SAMPAIO, José Adércio Leite, op. cit., p. 514.

72 .SAMPAIO, José Adércio Leite., op. cit., p. 514.

Para uma análise do tema, ver MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor, cit., p. 72-77.

73 .SAMPAIO, José Adércio Leite, op. cit., p. 516.

74 .COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais Comentada.* São Paulo: Ed. RT, 2018. p. 101.

75 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit., p. 9.

76 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit., p. 10.

77 .RODOTÁ, Stefano. *A vida na sociedade da vigilância,* cit., p. 59.

78 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit., p. 10.

79 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit., p. 10.

80 .Ainda segundo o mesmo dispositivo, “o princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados”.

81 .SAMPAIO, José Adércio Leite, op. cit., p. 509.

82 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit., p. 12.

83 .DE LUCCA, Newton; MACIEL, Renata Mota. A Lei 13.807, de 14 de agosto de 2018: a disciplina normativa que faltava cit., p. 45.

84 .SAMPAIO, José Adércio Leite, op. cit., p. 512.

85 .SAMPAIO, José Adércio Leite, op. cit., 513.

86 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit, p. 13.

87 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit, p. 13.

88 .MIRAGEM, Bruno. A Lei Geral de Proteção de Dados, cit., p. 14.

89 .A igualdade entre homens e mulheres é a regra, sendo a distinção a exceção. O tratamento excepcional deve vir da própria norma constitucional ou, quando vier de norma hierarquicamente inferior, a discriminação tem que ter respaldo em valores constitucionalmente protegidos. Não existe norma legal a justificar a distinção de preços entre homens e mulheres nos bares, restaurantes e casas noturnas. Não existe diferença entre homens e mulheres, que procuram os serviços desses estabelecimentos em igualdade de condições, que justifique do ponto de vista lógico a distinção de preços que está sendo praticada por alguns nesse segmento do mercado. (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2016, 2/2017/GAB-DPDC/DPDC/SENACON. Disponível em: [www.justica.gov.br/news/diferenciacao-de-precos-em-funcao-de-genero-e-ilegal/nota-tecnica-2-2017.pdf/view]. Acesso em: 03.02.2019.

Observe-se que o Judiciário brasileiro, mesmo por ocasião da sua vigência, já vinha afastando a aplicação dessa nota técnica. O juízo da 6ª Vara Federal da Seção Judiciária do Estado de Goiás

julgou procedente ação civil pública intentada pela Associação Brasileira de Bares e Restaurantes de Goiás, confirmando tutela de urgência deferida nos mesmos autos, para determinar que: "a ré [União] ou qualquer agência estatal integrante do sistema de proteção ao consumidor abstenha-se de autuar ou aplicar punições aos estabelecimentos associados à autora, em razão da Nota Técnica 2/2017/GAB-DPDC/DPDC/SENACON, bem como da Recomendação Conjunta feita pelo Ministério Público de Goiás, Procon Goiás e Procon Goiânia, ou de quaisquer atos regulamentares dessas fontes".

De forma semelhante, o juízo da 17ª Vara Cível Federal da Seção Judiciária do Estado de São Paulo julgou procedente o pedido em ação civil pública movida pela Associação Brasileira de Bares e Restaurantes de São Paulo, determinando que a ré (União) se abstenha de "autuar ou aplicar punições aos estabelecimentos associados à autora, em razão da Nota Técnica 2/2017/GAB-DPDC/DPDC/SENACON que dispõe sobre a ilegalidade na diferenciação de preços entre homens e mulheres". A mencionada sentença, que é de fevereiro de 2020, determinou a revogação da Nota Técnica 2/2017/GAB-DPDC/SENACON, abstenção na aplicação de penalidades administrativas, tendo transitado em julgado, encontrando-se o feito, atualmente, na fase de cumprimento de sentença. À mesma conclusão chegou o juízo da 8ª Vara de Fazenda Pública do Tribunal de Justiça do Rio de Janeiro, quando deferiu a tutela provisória para "determinar que as rés se abstenham de aplicar às sociedades empresárias substituídas multas e/ou quaisquer outras penalidades administrativas fundadas na diferenciação de preços por gênero".

Os Tribunais Superiores ainda não se manifestaram sobre a questão, mas, nos autos do Recurso Inominado 0718852-21.2017.8.07.0016, foi interposto recurso extraordinário, cujo agravo do artigo 1.042 do CPC/2015 (LGL\2015\1656), está em trâmite no STF, e já há parecer do MPF solicitando a análise do Plenário acerca de existência de repercussão geral. Caso a relevância de tema e a transcendência subjetiva sejam reconhecidas, o STF pode vir a pacificar a matéria.

90 .O que é reforçado pelos parágrafos do mesmo artigo 20 da LGPD: "§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais".

91 .ZANATTA, Rafael A.F.; SOUZA, Michel R.O. A tutela coletiva em proteção de dados pessoais: tendências e desafios. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de; MACIEL, Renata Mota. *Direito & Internet IV.* Sistema de Proteção de Dados Pessoais. São Paulo: Quarter Latin, 2019. p.411