INSTITUTO BRASILIENSE DE DIREITO PÚBLICO
ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM DIREITO
MESTRADO PROFISSIONAL EM DIREITO

FELIPE BOTELHO SILVA MAUAD

AS ATRIBUIÇÕES DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E O CONFLITO COM OUTRAS INSTITUIÇÕES: uma análise da atuação do órgão trazido pela Lei Geral de Proteção de Dados Pessoais

BRASÍLIA
2022

FELIPE BOTELHO SILVA MAUAD

AS ATRIBUIÇÕES DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E O CONFLITO COM OUTRAS INSTITUIÇÕES: uma análise da atuação do órgão trazido pela Lei Geral de Proteção de Dados Pessoais

Dissertação de Mestrado apresentada como requisito para obtenção do Título de Mestre em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

Orientador: Professor Dr. Gustavo Justino de Oliveira.

BRASÍLIA
2022

FELIPE BOTELHO SILVA MAUAD

AS ATRIBUIÇÕES DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E O CONFLITO COM OUTRAS INSTITUIÇÕES: uma análise da atuação do órgão trazido pela Lei Geral de Proteção de Dados Pessoais

Dissertação de Mestrado apresentada como requisito para obtenção do Título de Mestre em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

Orientador: Professor Dr. Gustavo Justino de Oliveira.

X/X/X

BANCA EXAMINADORA

_____

Prof. Dr. Gustavo Henrique Justino de Oliveira
USP – Universidade de São Paulo e IDP – Instituto Brasiliense de Direito Público

_____

Prof. Dr. Guilherme Pereira Pinheiro
IDP – Instituto Brasiliense de Direito Público

_____

Prof. Dr. André Castro Carvalho
USP – Universidade de São Paulo

AGRADECIMENTOS

Primeiramente, agradeço a Deus que, certamente, me auxiliou em diversos momentos da minha vida e sempre me deu forças para continuar na minha busca pelo desenvolvimento pessoal.

À minha noiva, Daniela, que, de forma compreensiva e altruísta, me apoiou e me deu forças para que fosse possível finalizar o curso de mestrado, mesmo que isso importasse em adiamento de diversos planos.

Aos meus pais, Antônio e Jacira, e ao meu irmão, Eduardo, pela minha formação moral e intelectual. Sem os valores por eles repassados, sem sombra de dúvidas, de nada valeria a caminhada até aqui realizada.

Ao meu amigo, Alex Augusto, o qual, de companheiro de escritório, se tornou um aliado de batalhas e ponto de apoio para momentos de aflição e dúvidas.

Ao meu orientador, Gustavo Justino, que aceitou a árdua tarefa de me orientar e, mesmo notando minhas inseguranças, me manteve focado e confiante no tema proposto. Os carinhosos “puxões de orelha” com relação às diversas alternâncias de capítulos, temas e subtópicos foram essenciais para que eu mantivesse meu foco e, consequentemente, conseguisse obter o presente substrato.

Com toda certeza, além do que restou agregado academicamente, carregarei esses ensinamentos atrelados a uma “autoconfiança” para a minha vida pessoal.

Por último, mas não menos importante, agradeço a todos os meus companheiros de Mudrovitsch Advogados, os quais me instigam a buscar o crescimento pessoal, profissional e intelectual, bem como me apoiam diariamente a ser sempre melhor.

RESUMO:

Os dados pessoais são, cada vez mais, objeto de atenção por parte dos mais diversos Estados. Tendo em vista essa crescente onda de preocupação, não há como se olvidar que surgiram, ao redor de todo o globo, diversas leis e normas que tratam dessa temática. No Brasil, visualizou-se no mundo jurídico a Lei nº. 13.709/18 que busca, justamente, proteger esse tipo de bem. Em que pese a ideia em questão, certamente, existirá controvérsia relacionada à competência Autoridade Nacional de Proteção de Dados, mormente com relação aos aspectos de conflito com outros órgãos e entidades. Nesse contexto, analisar-se-á o limite da atuação do órgão em pauta. Após a obtenção dessas informações, será formulada conclusão relacionada ao problema proposto.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais; Autoridade Nacional de Proteção de Dados Pessoais; Competência.

ABSTRACT:

Personal data is increasingly being addressed by the most diverse countries. Bearing in mind this concern, various laws and regulations have emerged around the globe about this topic. In Brazil, the Law nº. 13,709/18 seeks, precisely, to protect this type of asset. Regardless of the idea that has been brought, certainly, there will be controversy related to the competence of the National Data Protection Authority, especially about the conflict with other entities. In this context, the limit of the performance of the organ in question will be analyzed. After obtaining such informations, a conclusion related to the proposed problem will be formulated.

Keywords: Brazilian General Data Protection Law; National Data Protection Authority; Competence.

SUMÁRIO

INTRODUÇÃO

A ideia de conflito, em qualquer campo que seja, se assemelha muito a uma hipótese de confronto e choque. É dizer, diante de uma eventual problemática nesse sentido, ter-se-á dois indivíduos em uma dicotomia.

Trazendo-se para o Direito Administrativo, não são raras as situações em que dois órgãos, entes, ou entidades, simultaneamente, entendem que estão a cargo de uma análise extrajudicial acerca de uma determinada situação concreta.

Ora, é plenamente possível que duas autoridades administrativas se tenham como competentes, ou incompetentes, para desempenhar uma atividade em detrimento da atuação de outrem.

E isso, tendo em vista a necessidade de maior controle estatal das facilidades de coletas de dados provenientes da evolução informática (CASTELLS, 2006), poderá ocorrer no que tange ao escopo de atuação da Autoridade Nacional de Proteção de Dados, mormente porque a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) surgiu, dentre outros objetivos, com o intuito de complementar outras normas, como a Lei de Acesso à Informação, o Marco Civil da Internet, a Lei de Defesa da Concorrência e o Código de Defesa do Consumidor (MENDES; DONEDA, 2018, p. 469).

É dizer, parece claro, até mesmo tendo em vista esse intuito somatório da Lei n. 13.790/2018 e da busca em se atender a um direito que, com base na promulgação da Emenda Constitucional n. 115, é fundamental, que existirão normas regulamentares e fiscalizatórias provenientes de outras instituições que incidirão, ainda que conjuntamente ao que será disposto no futuro pela Autoridade Nacional de Proteção de Dados, sobre eventuais problemáticas que envolvam a temática “proteção de dados” (PINHEIRO; SOUTO; MORAES, 2019).

A título ilustrativo, pode-se mencionar que notas técnicas provenientes da Secretaria Nacional do Consumidor (Senacon) e resoluções provenientes do Banco Central (Bacen), do Conselho Administrativo de Defesa Econômica (CADE), da Receita Federal e, ainda, da Agência Nacional de Saúde Suplementar (ANS), certamente, dividirão espaço com as regulamentações que serão estabelecidas pela Autoridade Nacional de Proteção de Dados.

Ora, a defesa dos dados pessoais possui um caráter interdisciplinar e multissetorial, de modo que a matéria em pauta é “abarcada” por diversos ramos do direito.

Esse fato faz com que o cotejo do referido direito seja tido como “transversal” e tomado por uma “ubiquidade”, eis que os seus contornos serão encontrados em mais de um corpo

normativo e em um espaço amplo (principalmente, por se tratar, em diversas oportunidades, de um espaço virtual).

O que se coloca é que, considerando que várias das pessoas e órgãos regulados pelas instituições supracitadas exercem verdadeiras atividades empresariais envolvendo o tratamento de dados pessoais, poderão surgir situações em que um mau uso daqueles bens jurídicos será fiscalizado tanto na esfera da Lei n. 13.709/2018 quanto nas esferas de outras legislações e normas.

Tal circunstância pode trazer uma atuação conflitante entre o órgão de proteção de dados pessoais e os órgãos de proteção com o viés consumerista, econômico, financeiro, dentre outros.

Justamente por isso é que o presente trabalho é apresentado; eis que, tendo-se em mente que a segurança jurídica deve ser buscada e, também, que o *bis in idem* não é aceito pelo ordenamento jurídico pátrio, há patente importância em se esclarecer, da forma mais cristalina possível, ao questionamento "como evitar uma dupla penalização (*ne bis in idem*) de uma pessoa que atue em desacordo com as premissas protetivas dos dados pessoais?".

Em relação à organização da pesquisa, tem-se três pilares. No primeiro capítulo deste substrato acadêmico, partiu-se das ideias de transversalidade para se destacar que a interdisciplinaridade da discussão afeta aos dados pessoais, bem como para evidenciar os conceitos dos bens jurídicos protegidos pela Lei Geral de Proteção de Dados Pessoais.

Afinal, sem este primeiro exame, não poder-se-ia entender no que consistem as operações que se encontram sob a tutela fiscalizatória e normativa da Autoridade Nacional de Proteção de Dados.

Posteriormente, adentrando-se ao segundo capítulo deste trabalho, em especial com o fito de verificar as suas funções e os seus poderes administrativos, foi trabalhado o processo legislativo que culminou na criação e nas características do órgão de proteção de dados.

A partir daí, foi sopesado se algumas premissas de atuação observadas na norma se tratariam de *third party verification*, autorregulação regulada e *soft law*. Em outros termos, buscou-se esmiuçar a origem e as atribuições legalmente trazidas à Autoridade Nacional de Proteção de Dados.

No terceiro capítulo, destacou-se, tendo-se em mente a jurisprudência que o transplantou para o ordenamento jurídico pátrio, os aspectos históricos e modernos do princípio do *bis in idem*.

Ademais, conforme extraído dos ensinamentos de José Cretella Júnior, serão tratadas as diferenças entre os conceitos de "conflito de competência" e "conflito de atribuições" no

intuito de aproximar as prerrogativas dadas à Autoridade Nacional de Proteção de Dados das atuações exercidas por outros órgãos e instituições administrativas com funções normativas e fiscalizatórias que envolvam, mesmo que de forma indireta, o tratamento de dados pessoais. Assim, tentou-se iluminar a problemática afeta a uma atuação simultânea entre aqueles órgãos e pessoas e a Autoridade Nacional de Proteção de Dados Pessoais.

Como se nota, portanto, institutos provenientes de outros países serão mencionados neste trabalho, mas apenas com o espeque de facilitar a visualização da conclusão obtida. Nesse contexto, tais conceitos estrangeiros não fizeram, ao menos de forma aprofundada, parte da pesquisa realizada.

Ao final, apresentar-se-á conclusão para estabelecer soluções que evitem com que a atuação da Autoridade Nacional de Proteção de Dados seja questionada, em especial mitigando a existência de alegações de conflito de atribuição com outros órgãos e entes do Poder Público.

1 DA DEFESA DOS DADOS PESSOAIS

Não há como se olvidar que situações definidas em uma seara do Direito, quando possível, podem e devem ser aproveitadas por outros nichos.

Isso ocorreu, por exemplo, nas hipóteses em que princípios inerentes ao Direito Penal, tal qual o da não culpabilidade, passaram a ser englobados no âmbito do Direito Administrativo (JUSTEN FILHO, 2015, p. 596) e, consequentemente, deu-se vida a um pensamento no sentido de que o Estado, almejando uma ampla observância aos direitos fundamentais, deve receber os estímulos de uma determinada sociedade para satisfazê-los da forma mais célere e ideal possível (OLIVEIRA, 2008, p. 83).

Notadamente, portanto, a perspectiva em pauta muito se assemelha à conhecida "transversalidade" proveniente e trabalhada no âmbito do Direito Ambiental e que permitiu com que:

> De lá para cá, são incontáveis as obras de Direito Ambiental publicadas, conferindo maior solidez teórica à matéria. Isso tudo, por sua vez, conduziu à autonomia (sempre relativa!) do Direito Ambiental em face das demais disciplinas jurídicas, bem como a sua inclusão nos programas dos cursos de direito pelo Brasil afora. Mas a revolução jurídica "verde" a que nos referimos anteriormente não para por aí. O Direito Ambiental, por sua natureza dinâmica e transversal (Querschnittsrecht), também acabou por influenciar e reformular o conteúdo de institutos vinculados tradicionalmente a outras disciplinas jurídicas. A título de exemplo, podemos citar a função ecológica que passou a conformar o conteúdo do direito (e dever) de propriedade, consagrada expressamente no art. 1.228, § 1º, do Código Civil de 2002, também como reação ao disposto no texto constitucional de 1988. O Direito Ambiental, nesse contexto, passou a dialogar conceitual e normativamente com os diversos ramos jurídicos, a fim de "esverdear" o Direito como um todo e fazer com que os direitos (e princípios) ecológicos migrassem para o centro do nosso sistema jurídico, ao lado da liberdade, da igualdade, da dignidade da pessoa humana, do ideal de justiça etc. (SARLET; FENSTERSEIFER, 2014, p. 34 – 35)

Ou seja, a evolução do Direito, até mesmo considerando a interpretação sistemática em que o ordenamento jurídico pátrio é tratado como se um só fosse (MAXIMILIANO, 2011, p. 100), faz com que institutos, comumente aplicados a uma determinada seara jurídica, se possível, sejam irradiados para outros ramos.

Certamente, a Lei n. 13.709/2018 deverá ser cotejada por meio desse olhar mais integrativo.

Afinal, não há como se olvidar que aquela normativa, ao fim e ao cabo, possui o escopo de permitir com que um direito fundamental seja atendido. É que, com o advento da Emenda Constitucional n. 115, alçou-se a defesa dos dados pessoais a um direito de grande lavra. Confira-se:

> Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:
>
> "Art. 5º .....
> .....
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.
> ..... (BRASIL, 2022)

Bem verdade, portanto, o próprio surgimento da Lei Geral de Proteção de Dados foi proveniente do não atendimento, ao menos na totalidade, pelas normativas e legislações que lhe são anteriores acerca da ideia de proteção dos dados pessoais como um direito fundamental integrante dos direitos da personalidade (MENDES, 2014).

Em outros termos, aquelas hipóteses protetivas mais antigas não atingiram, com perfeição, a proteção almejada das informações encontradas na realidade física e, também, deixaram a desejar no que tange ao controle dos dados pessoais existentes no ciberespaço, qual seja, o plano virtual povoado por informações trocadas entre computadores (FORTES; BOFF, 2016).

Outrossim, por meio da Lei Geral de Proteção de Dados Pessoais, se teve um importante adendo a diversos conceitos e institutos incipientemente previstos em outras normas, mesmo porque, outrora, praticamente toda celeuma que envolvia a questão de mau uso do bem jurídico aqui iluminado era solucionada tão somente por meio da aplicação de princípios gerais (PESTANA, 2019).

Obviamente, aqueles preceitos não serão, simplesmente, abandonados, mas contarão com elementos que permitirão uma aplicação de suas inteligências de uma forma mais específica e cirúrgica.

Isso porque, atualmente, encontram-se melhor definidos diversos conceitos que são abordados na norma, inclusive, a própria ideia de “dados”, bem como no que tange às medidas que serão tomadas para proteger esse bem jurídico. Além do mais, é certo que, por meio da promulgação da Emenda Constitucional n. 115 (BRASIL, 2022), a defesa dos dados pessoais foi, de uma forma direta, alçada à categoria de direito fundamental.

Nessas conjunturas, com o fito de permitir uma clara observância da problemática trazida ao debate, é interessante se destacar as evoluções e inovações trazidas pela nova norma e cotejá-las com o que já se tinha em outros campos normativos.

1.1 Os tipos de dados previstos pela Lei Geral de Proteção de Dados Pessoais

Ao longo dos anos, a sociedade transitou por diversas formas de organização de economia. Afinal, já tivemos nações cujas atividades econômicas estavam vinculadas à agricultura, outras com lastro na disponibilização de serviços e bens materiais e, agora, o que se tem visto é o crescimento de uma economia cujo embasamento consiste na disponibilização de serviços e bens tecnológicos (BIONI, 2019, p. 33 – 34).

Diante deste novo tipo de composição econômica lastreada na tecnologia, percebeu-se que os dados, utilizando-se da gama disponível *online* para a sua compreensão, teriam um alto valor e um amplo mercado (ZUBOFF, 2015).

A força desse tipo de atividade empresarial, aliás, fez com que alguns estudiosos defendessem o surgimento de uma forma de economia denominada de *infonomics*, ou seja, um método de giro de capital que tem a informação como o seu principal ativo (LANEY, 2011) e que é capaz de permitir com que:

> Grandes empresas de tecnologia da internet, como o Google, coletam dados pessoais dos usuários de seus serviços, para fins comerciais, principalmente. Os dados são tratados com o auxílio de métodos estatísticos e técnicas de inteligência artificial, com o fim de sintetizar hábitos, preferências pessoais e outros registros. A partir disso são criados perfis para cada usuário (profiling) que possibilitam o envio seletivo de mensagens publicitárias de um produto a seus potenciais compradores (SILVA, 2019, p. 57).

É dizer, tendo em vista as melhorias provenientes dos avanços da coleta de dados e informações através da *internet*, que houve uma necessidade de se controlar o conhecimento acerca do comportamento de uma determinada pessoa que acaba, de certa forma, sendo disponibilizado às grandes empresas (TOMASEVICIUS FILHO, 2020).

Por conta disso, entendeu-se que os dados pessoais careceriam de um olhar mais cauteloso por parte do Estado. Isso porque aqueles bens jurídicos podem trazer uma ampliação da identidade humana no âmbito virtual e, por essa razão, devem ser tratados como uma verdadeira extensão da personalidade de um sujeito (MENDES, 2011, p. 75).

Obviamente, existem diversos tipos de dados circulando no ciberespaço. Contudo, somando-se ao que trouxe o Marco Civil da Internet para o âmbito virtual, a Lei Geral de Proteção de Dados Pessoais possui o escopo de controlar, especificamente, aqueles elementos informativos que se relacionem a um determinado administrado.

Portanto, com o fito de elucidar o objeto de tutela da lei em comento, o legislador separou os dados nas categorias de “dados pessoais”, “dados pessoais sensíveis” e “dados anonimizados”.

Apenas aqueles dados com a característica de “pessoais” receberão uma guarida

estatal, sendo interessante destacar-se as diferenças dos tipos indicados na legislação.

1.1.1 *Os dados pessoais*

Os dados pessoais são elementos primitivos que permitem com que um agente obtenha uma informação acerca de uma pessoa (WACKS, 1989, p. 25 – 26). É dizer, se está diante de uma figura que antecede a algo mais aprofundado e passível de comunicação, recebimento e entendimento por outrem (DONEDA, 2011, p. 94).

Corolário lógico, até em razão da inteligência do artigo 5º, I, da Lei n. 13709/2018, os dados pessoais são amplos e podem consistir em qualquer colocação e indicação que permita com que uma pessoa natural seja identificada no mundo virtual e real (CELANO; ESPERATO; 2020).

Além desses dados que, de plano, fazem com que uma determinada pessoa natural seja identificada, há de se pontuar que os elementos que podem, por meio de um somatório proveniente do grande volume e variedade existentes nos meios eletrônicos e físicos, fazer com que uma determinada pessoa seja reconhecida, também, são considerados dados pessoais (HIJMANS, 2016, p. 98).

Diz-se isso, porquanto essa junção de diversos dados, muitas vezes até fornecidos espontaneamente pelo seu detentor, tem se mostrado ainda mais valiosa do que um mero fragmento de informação que restou disponibilizado sem uma base tão estruturada (KALYVAS; OVERLY, 2015).

Desse modo, podemos considerar dados pessoais os fatos, comunicações e atos que possam revelar características de uma pessoa natural que estejam vinculadas à personalidade, etnia, relações pessoais, domicílio, opinião política, orientação sexual, dentre outras (RODOTÀ, 2008, p. 6).

1.1.2 *Os dados pessoais sensíveis*

Ainda dentro da ideia de “dados pessoais” (DONEDA, 2006, p. 160), concluiu-se que certos elementos capazes de ensejar a obtenção de uma informação acerca de um indivíduo, por trazerem um maior risco aos direitos da personalidade e serem capazes de gerar uma discriminação indesejada, deveriam ser tidos como uma figura qualificada (MENDES, 2008, p. 62).

São, basicamente, aquelas noções que envolvem convicções filosóficas e políticas,

saúde, vida sexual, religião, etnia, dados genéticos, dados biométricos, posição partidária ou sindical (ASCENSÃO, 2010, p. 105).

Novamente, há de se chamar atenção para a possibilidade de um tratamento conjunto de diversos dados ser capaz de gerar uma informação relacionada às temáticas em questão. A propósito:

> Para além do problema da discriminação, dois outros problemas podem aparecer com o *data mining*, à luz da teoria da proteção de dados pessoais. O primeiro deles diz respeito ao descumprimento do princípio da finalidade, na hipótese em que a finalidade da mineração de dados não tenha ficado clara para o consumidor ou não tenha sido apresentada pela empresa. O segundo diz respeito à possibilidade de que essa técnica de mineração de dados possa transformar dados, à primeira vista inofensivos, em informações sensíveis que revelem informações do consumidor sobre as quais ele esperava sigilo [...] (MENDES, 2008, p. 104).

Portanto, o que se tem é que, dentro dos dados pessoais, existe uma categoria de elementos relacionados a um administrado que merecem uma maior atenção, tanto o é, aliás, que o tratamento e a utilização deste tipo de dados, nos termos do artigo 11, da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), é feito apenas em casos específicos, ou, mediante um consentimento qualificado.

1.1.3 *Os dados anonimizados*

O último tipo de dados mencionado no bojo da Lei Geral de Proteção de Dados Pessoais é o anonimizado. Está-se, aqui, defronte à antítese dos dados pessoais, porquanto estes elementos são inaptos a revelar uma pessoa natural e, conseguintemente, não identificam um nome ou imagem de um indivíduo (BIONI, 2020).

Existe, dessa forma, um processo que rompe o vínculo entre os dados fornecidos e o seu titular (DONEDA, 2006, p. 44) para evitar com que o denominado “espião de dados” os acessem (DUNCAN; KELLER-MCNULTY; STOKES, 2001). Esse processo pode se dar por meio de generalização, supressão, encriptação embaralhamento e mascaramento, os quais podem ser definidos da seguinte maneira:

> As técnicas atualmente existentes para a proteção de dados, (generalização, supressão, embaralhamento e perturbação), propostas pela comunidade acadêmica, podem ser utilizadas e/ou combinadas com o objetivo de anonimizar os dados. Essas técnicas são apresentadas a seguir:
> a) Generalização: para tornar o dado anônimo, esta técnica substitui os valores de atributos semi-identificadores por valores menos específicos, mas semanticamente consistentes, que os representam. A técnica categoriza os atributos, criando uma

> taxonomia de valores com níveis de abstração indo do nível particular para o genérico. Como exemplo, podemos citar a generalização do atributo Código de Endereçamento Postal (CEP), o qual pode ser generalizado de acordo com os seguintes níveis: CEP (60.148.221) > Rua > Bairro > Cidade > Estado > País.
> b) Supressão: esta técnica exclui alguns valores de atributos identificadores e/ou semiidentificadores da tabela anonimizada. Ela é utilizada no contexto de bancos de dados estatísticos, onde são disponibilizados apenas resumos estatísticos dos dados da tabela, ao invés dos microdados [Samarati 2001].
> c) Encriptação: esta técnica utiliza esquemas criptográficos normalmente baseados em chave pública ou chave simétrica para substituir dados sensíveis (identificadores, semiidentificadores e atributos sensíveis) por dados encriptados.
> d) Perturbação (Mascaramento): esta técnica é utilizada para preservação de privacidade em data mining ou para substituição de valores dos dados reais por dados fictícios para mascaramento de bancos de dados de testes ou treinamento. A idéia geral é alterar randomicamente os dados para disfarçar informações sensíveis enquanto preserva as características dos dados que são críticos para o modelo de dados. Duas abordagens comuns desta técnica são a randomização (Random Data Perturbation - RDP) e a condensação dos dados [Chen and Liu]. (MONTEIRO; MACHADO; BRANCO JR, 2014, p. 53 – 54)

Apesar de existirem todos os métodos evidenciados, não há como se olvidar que a anonimização deve ser sempre buscada com base em uma irreversibilidade (BASSO; MATSUNAGA, 2016, p. 164 – 171).

Nesses contornos, o processo de anonimização deve antecipar todo um contexto em que se tenha em mente uma impossibilidade, ainda que futura, de regressão e, dessa forma, de tolher-se o anonimato pretendido, ainda que se reconheça, até mesmo considerando a rápida evolução dos meios tecnológicos, que se atingir essa ideia de "eficiência total" é quase impossível (NARAYANAN; SHMATIKOV, 2010, p. 24). Ou seja, por mais que tenha havido um procedimento de anonimização dos dados pessoais fornecidos por um determinados usuário, sempre existirá o risco de que aquele meio seja superado e, assim, de que um dado que outrora seria tido como "anônimo" se torne um dado pessoal (TENE, 2013, p. 1.242).

Exatamente, por esse motivo, é de grande importância que se evite que a utilização da *big data* reverta a anonimização aplicada por um determinado tratador de dados pessoais (GUARIENTO; MARTINS, 2020). E isso é extremamente complexo; eis que, tendo em vista, por exemplo, as melhorias tecnológicas que permitiram com que um conteúdo *online* seja acessado rapidamente por meio de aparelhos celulares (PUGLIESI; BRANDÃO, 2015, p. 455), cada vez se tem uma maior quantidade de dados nos meios digitais (SCHROEDER, 2018, p. 127).

Nos dias atuais, portanto, ficou mais fácil unir pequenos eventos da vida digital para fins de se obter um extrato de alto valor, de modo que até mesmo elementos sem uma aparente importância permitiriam com que se obtivesse uma informação acerca de uma pessoa natural (FISHER et al., 2012, p. 53).

Dessa união de volumes de dados estruturados, e também não estruturados, é que as empresas podem chegar a uma conclusão, analisar o comportamento dos seus usuários e, por consequência, transformar um dado que outrora seria "inútil" em "útil" (AKERKAR; HONG, 2018, p. 4 – 5).

Nesses contornos, sempre há de se ter uma cautela para que, através do uso de multiplicidade de fontes, não seja perdido o procedimento de anonimização utilizado e se tenha uma reversão do método desvinculativo aplicado (COTS; OLIVEIRA, 2018, p. 93).

Assim, apesar de, *a priori*, os dados anonimizados não terem a guarida da Lei Geral de Proteção de Dados Pessoais, a Autoridade Nacional de Proteção de Dados deve se manter alerta para uma eventual alteração da característica daquilo que se disponibilizou, especialmente, nos meios *online*.

1.2 As operações que se encontram sob o enfoque da Lei Geral de Proteção de Dados Pessoais

Estabelecido o conceito dos "dados pessoais" protegidos e melhor evidenciados pela Lei n. 13.709/2018, há que se trabalhar as operações que são o enfoque da norma e, também, da Autoridade Nacional de Proteção de Dados.

Nesse espeque, a principal atividade a ser regulada e monitorada pelo órgão em pauta é o tratamento de dados. A ideia em tela é ampla e engloba atividades empresariais e governamentais que envolvam os dados pessoais, tais quais, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

O rol em questão, por certo, encontra-se aberto para eventuais acréscimos de atividades, especialmente ao se notar que o próprio inciso X, do artigo 5º, da Lei Geral de Proteção de Dados Pessoais, prevê, genericamente, que o tratamento sob guarida da norma é "toda operação realizada com dados pessoais".

Ou seja, são diversas as hipóteses em que os operadores e controladores dos dados, aqueles que manuseiam e tomam decisões a respeito desses bens, deverão, nos termos do artigo 37 da lei em pauta, manter registradas para denotar uma atuação escorreita de sua parte.

Qualquer que seja a atividade que envolva dados pessoais, exige-se o pleno respeito aos princípios norteadores e requisitos necessários à realização do tratamento de tais bens jurídicos (BRASIL, 2018, arts. 6º e 7º).

Destarte, caso não haja a devida observância a qualquer um desses pontos, abrir-se-á um espaço para que a Autoridade Nacional de Proteção de Dados exerça suas atribuições, o que denota a necessidade de se abordar essas questões que somente vieram a se consolidar com o surgimento e vigência da recente legislação.

1.2.1 *Dos princípios básicos norteadores do tratamento de dados*

Antes mesmo da existência da Lei Geral de Proteção de Dados Pessoais, havia uma concordância global, a qual recebeu o nome de *"Fair Information Principles"*, relacionada à uma necessidade de que as operações de tratamento de dados se pautassem em um quadro principiológico (MENDES, 2014, p. 68).

Esses ideais foram reproduzidos em território nacional, eis que a nossa legislação protetiva de dados pessoais se embasou em estudos, pesquisas, leis e normas que já levavam em consideração esses preceitos estabelecidos, ainda na década de 70, em outros países (REINALDO FILHO, 2018).

Em razão disso, o tratamento de dados no Brasil deve ocorrer com base nos cânones de boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e, por fim, da responsabilização e prestação de contas (BRASIL, 2018, art. 6º).

1.2.1.1. Dos princípios da boa-fé, finalidade e adequação

O princípio da boa-fé faz com que, no âmbito do tratamento de dados, exista uma relação pautada em dois prismas. O primeiro é caracterizado por uma boa intenção dos agentes e, portanto, de inexistência do intuito de se causar dano (CORDEIRO, 2013, p. 510). O segundo, por sua vez, consiste na existência de boa vontade de interpretação tanto no estabelecimento de direitos e deveres quanto nos decotes de liberdades propostos (JUNQUEIRA DE AZEVEDO, 2000, p. 4 – 6).

Visando uma atuação de boa-fé, não pode uma empresa que trabalhe com alienação de mercadorias, por exemplo, tratar e vender, após a finalização de um contrato ali firmado, os dados de um cliente (FLUMIGNAN; FLUMIGNAN, 2020, p. 126).

Já por meio do princípio da finalidade, buscou o legislador fazer com que o tratamento de dados pessoais somente fosse realizado para se atingir propósitos específicos, legítimos e informados, claramente, ao titular. Sobre o tema:

> O primeiro dos princípios eleitos pela LGPD é o da finalidade. O normativo o define como a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
> Por propósitos legítimos, quer se referir a uma finalidade movida pelo bom senso, razão, legalidade, bons costumes e boa fé, distanciando-se, portanto, da iniciativa subalterna, emulativa, emocional, ilícita e de má fé.
> Refere-se a propósitos específicos, por enfatizar a preocupação de que o tratamento se volte, certeiramente, para um objetivo determinado relevante para o ser, como se dá ao procurar minorar as repercussões do infarto ou de prolongar a vida no espaço sideral.
> Já por propósitos explícitos procura enfatizar o aspecto unívoco do tratamento, ou seja, não admitindo a equivocidade ou ambiguidade. Em outras palavras, tendo o objetivo clara e previamente delineado, não permitindo que dúvidas possam surgir após ser especificado seu conteúdo.
> Todos esses objetivos que, integradamente, conformam a finalidade admitida pelo normativo, devem ser informados ao titular, o qual, com ele concordando, delimitará o objeto do tratamento, domínio esse que não poderá ser subsequentemente alterado, salvo se nova, e expressa concordância for obtida desse titular. (PESTANA, 2019)

Dessa forma, tendo em vista que o princípio em tela vincula o operador ao cumprimento do objetivo pretendido, a finalidade acaba se comunicando com o próprio princípio da boa-fé (LIMA, 2015, p. 1 – 24).

Diz-se isso, pois a empresa que solicita os dados com a indicação dos motivos para o fazer não pode, posteriormente, alterar o escopo da utilização daqueles bens. Ou seja, não é permitido, exemplificando, uma empresa solicitar o e-mail de um usuário para confecção de *login* e o utilizar, posteriormente, para enviar ofertas (FLUMIGNAN; FLUMIGNAN, 2020, p. 128).

Evita-se, desse modo, que se tenha uma declaração de vontade genérica que dê plenas liberdades de uso ao operador de dados, tal qual um cheque em branco (SOLOVE, 2013, p. 1884).

Complementando os dois princípios supracitados, tem-se o princípio da finalidade, porquanto está-se diante da ideia de que o tratamento de dados apenas pode ocorrer quando houver uma compatibilidade da informação contida no pedido de fornecimento apresentado pelo operador e o que efetivamente está sendo aplicado. Exatamente por essa razão é que uma pessoa jurídica que receba, consentidamente, dados cardíacos do relógio inteligente de um usuário para dar *feedback* não poderia lhe oferecer produtos de saúde (VAINZOF, 2019, p. 135).

Bem verdade, portanto, deve existir uma lógica entre o tratamento e o fim pretendido, entre o tratamento e aquela comunicação repassada ao usuário e entre o fim buscado e aquilo que foi indicado ao usuário (PESTANA, 2019).

Como exemplos de malferimento da adequação, Márcio Cots e Ricardo Oliveira (2018,

p. 101) suscitam uma destinação transviada dos dados, uma falsa alegação de que os dados obtidos serão eliminados e, por fim, se informar que haverá uma anonimização dos dados pessoais e, em realidade, ter-se apenas uma pseudoanonimização.

A grosso modo, sob a perspectiva do Direito Administrativo, poder-se-ia fazer uma analogia entre a adequação e a teoria dos motivos determinantes, cuja premissa consiste em trazer-se uma vinculação entre o fundamento de um ato administrativo e a sua validade (ARAUJO, 2006, p. 459).

Portanto, o que se tem é que, agindo com lealdade, aquele que solicita os dados de outrem deve informar o detentor daqueles bens e, obviamente, seguir aquilo que prometeu, sob pena de invocar um desrespeito ao que discorre a norma e podendo chamar para si uma sanção a ser aplicada pela Autoridade Nacional de Proteção de Dados.

1.2.1.2. Do princípio da necessidade

O ideal da necessidade diz respeito a reduzir, o máximo possível, o processamento dos dados pessoais, de modo que apenas sejam coletados e tratados bens que tenham ligação com as finalidades pretendidas e que tenham uma abrangência pertinente e não excessiva com relação ao que se busca (HOEPMAN, 2019, p. 26).

A regra da Lei Geral de Proteção de Dados Pessoais é, com efeito, o não tratamento dos dados e, caso seja importante que ocorra tal procedimento, deve haver um foco apenas nos dados que sejam imprescindíveis para o fim almejado (PESTANA, 2019). Na hipótese de serem colhidos dados que superam aquilo que seria imperioso ao negócio proposto, por certo incorrerá o agente coletor em um abuso de direito (SANTOS; TALIBA, p. 2–3).

1.2.1.3. Dos princípios do livre acesso aos dados e qualidade dos dados

O princípio do livre acesso aos dados se relaciona com o pensamento de que deve ser permitido que o titular consulte, gratuitamente, o banco de dados que possua suas informações armazenadas para obter cópias (SAMPAIO, 1997, p. 509).

Por conta disso, a premissa do livre acesso de dados se comunica com o cânone da qualidade dos dados.

Isso porque, apenas por meio do acesso é possível se notar e evitar erros quanto aos dados de um determinado usuário e, por consequência, afastar celeumas inerentes a um equívoco (MALETIC; MARCUS, 2000). Ou seja, não se coaduna com a existência de dados

pessoais inverídicos e não atuais relacionados a uma pessoa natural, mesmo porque evitar-se problemas acerca de informações é muito mais barato e simples que se detectar um problema dessa natureza e resolvê-lo (DALCIN, 2004).

1.2.1.4. Dos princípios da segurança, prevenção e da não discriminação

O ideal da segurança exige que uma determinada organização, que se utilize de dados de pessoas naturais, adote técnicas para protegê-los de acessos não autorizados e de destruição, perda, difusão e modificações indesejáveis, sob pena de que o controlador e operador dos dados indenize o titular e, dependendo do caso, responda criminalmente (MAGALHÃES; PESSOA, 2020, p. 295).

Ainda pretendendo com que o manejo dos dados ficasse no campo da licitude, previu-se os princípio da prevenção e da não discriminação.

O primeiro trouxe, em suma, uma perspectiva de tomada de cuidados para fim de prestigiar, sempre que possível, a privacidade (VAINZOF, 2019, p. 150). Ou seja, impõe-se com que os sistemas, as prátcas comerciais, os produtos, projetos e qualquer outra solução que englobe o manuseio dos dados pessoais sejam planejados para proteger os dados pessoais dos usuários (CAVOUKIAN, 2009).

E nem poderia ser diferente, porquanto, considerando que o extravio e mau uso de tais bens é potencializado por meio da velocidade e capacidade da *internet*, se torna extremamente difícil um retorno ao *status quo ante* (FLUMIGNAN, 2018, p. 35).

O segundo, por sua vez, tem o intuito de impedir com que a utilização de dados pessoais, os quais, muitas vezes, revelam valores que ultrapassam a figura da privacidade em sentido estrito e são sensíveis, tenha a ideia de trazer abusos e permitir com que se privilegie um grupo de pessoas em desfavor de outro (SARTORI, 2016, p. 63).

1.2.1.5. Do princípio da transparência

Justamente para efetivar os demais princípios elencados na norma, a Lei Geral de Proteção de Dados Pessoais previu que às relações tuteladas em seu bojo aplicar-se-ia o princípio da transparência (VAINZOF, 2019, p. 160).

Através da observância de tal princípio, tem-se que os controladores de dados, diante das dificuldades de se visualizar o poder dos dados pessoais e um aumento da vulnerabilidade nos meios virtuais, devem sempre considerar os usuários como a parte mais fraca da relação

(LEITE; LEMOS, 2014, p. 484–485), o que dá ensejo ao dever de trazer, sob a perspectiva de criar-se uma confiança no que foi solicitado (LUHMAN, 2005, p. 53), uma informação clara, completa e didática àqueles que lhes fornecerão tais bens jurídicos.

1.2.1.6. Do princípio da responsabilização e da prestação de contas

Por fim, considerando os tratamentos de dados, a Lei Geral de Proteção de Dados Pessoais prevê o princípio da responsabilização e da prestação de contas. Segundo a inteligência em questão, os controladores e operadores de dados devem cumprir, fielmente e eficazmente, as normas da lei e atender o que lhes é exigido pelo legislador, sob pena de serem responsabilizados e penalizados (VAINZOF, 2019, 178).

O princípio em pauta visa esclarecer que a matéria da proteção de dados pode ensejar em uma responsabilidade civil, mormente porque tal figura tem tanto uma natureza restaurativa quanto preventiva (ROSENVALD, 2017, p. 32). E, considerando-se que a tendência é a informatização da Administração Pública com uma natural disponibilização aos entes e órgãos governamentais de dados pessoais (e sensíveis), e que o artigo 42 da Lei Geral de Proteção de Dados Pessoais remete ao artigo 927 do Código Civil, sequer poderia ser diferente, de modo que o agente apenas não será responsabilizado quando demonstrar que não realizou o alegado tratamento equivocado, não atuou fora da legalidade (inexistiu ilicitude) ou que o dano foi proveniente de culpa do titular dos dados (PEREIRA; ALVIM, 2020, p. RB-45.6)

Nessas conjunturas, cumpre aos controladores e operadores de dados não apenas tomarem os devidos cuidados para com os bens que lhes foram entregues, mas também manter evidências das medidas adotadas. Por tal motivo, as pessoas que lidam com dados pessoais deverão contratar consultorias especializadas, ter protocolos de segurança efetivos e guardar relatórios das suas atividades para prestarem, quando instadas pela autoridade fiscalizadora, informações (FLUMIGNAN; FLUMIGNAN, 2020, p. 137).

1.2.2 ***Dos requisitos específicos para o tratamento de dados pessoais***

Observados os princípios estabelecidos na norma, é certo que a Lei Geral de Proteção de Dados Pessoais ilustra as situações em que poderá existir o tratamento dos bens ali tutelados. A primeira delas é a hipótese em que se tem um consentimento do titular dos dados (BRASIL, 2018, art. 7º).

O que existe é uma possibilidade de que, por meio de um aceite livre, específico, informado e demonstrável (PEREIRA, 2020, p. 83), um determinado titular de dados pessoais permita, dispondo da sua autonomia da vontade, que uma empresa, órgão, ou ente, realize o tratamento dos bens jurídicos que lhe pertencem. Nessa toada:

> O consentimento do interessado para o tratamento de seus dados é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais; através do consentimento, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos deste consentimento à natureza dos interesses em questão (DONEDA, 2006, p. 371).

Ao suscitar um consentimento livre, o legislador pretendeu fazer com que o titular dos dados tivesse escolha acerca da entrega de suas informações. Ou seja, a idea fulcral da liberdade estabelecida na norma diz respeito a uma disponibilização de diversas opções de escolha para que o titular dos dados possa analisar o que lhe foi oferecido e, assim, selecionar o caminho que julgue mais adequado para o seu bem estar (BIONI, 2019, p. 197).

Tal liberdade, por certo, busca evitar com que se tenha o enquadramento do tratamento de dados em uma relação baseada em um *take it or leave*. Em outros termos, afasta-se uma premissa em que se tem apenas duas opções a uma das partes que participa do negócio jurídico, quais sejam, aceitar as condições que lhe são impostas, ou, não aceitá-las e, portanto, não seguir com o pacto buscado (TARTUCE, 2020).

Por sua vez, o consentimento informado mencionado na Lei Geral de Proteção de Dados Pessoais busca fazer com que, não obstante existirem dificuldades naturais para que um usuário tenha o mesmo conhecimento temático que aquele possuído pelo fornecedor de serviços que envolvam os dados pessoais, haja uma clara e inteligível indicação das características afetas aos pedidos de entrega de informações. Isso porque, para que exista um convencimento hígido é necessário se fazer menção dos exatos contornos que envolvem a solicitação que restou apresentada (BIONE, 2019, p. 192 – 193).

Da mesma forma, adentrando-se na exigência de ter-se um consentimento específico, não basta com que se tenha uma solicitação geral e abstrata para fins de entrega e utilização de dados pessoais (BIONE, 2019, p. 198).

Ora, para que se considere um consentimento como sendo específico, deve haver a indicação do dado em especial que será utilizado em uma determinada operação. Ademais, por conta dessa inteligência normativa, o solicitador deve ter, a cada nova tentativa de acesso aos dados pessoais de um usuário, um aval (UNIÃO EUROPEIA, 2013, p. 14).

Acerca da ideia de que o aval fornecido pelo titular dos dados seja demonstrável, é

interessante pontuar que a Lei Geral de Proteção de Dados Pessoais fez constar em seu artigo 8º que o "consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (BRASIL, 2018). É dizer, trouxe-se uma exigência de que exista um documento apto a ilustrar o aval fornecido pelo titular dos dados, seja através dos meios convencionais, como um contrato ou formulário de papel firmado a mão, ou, por meios mais modernos, tal qual um documento assinado digitalmente (LIMA, 2019, p. 188).

Além de ser imperiosa a presença de todas essas características no bojo do consentimento ofertado pelo titular dos dados, não há como se olvidar que a concordância apresentada pode ser, a qualquer tempo, revogada (BRASIL, 2018, art. 8º, §5º). Portanto, o legislador compreendeu que, assim como existe uma facilidade para que o titular dos dados os forneça, dever-se-ia ter um método simples para que se cancelasse esse consentimento, sendo certo, todavia, que essa revogação não significa uma imediata eliminação dos dados, a qual somente será atingida com solicitação específica nesse sentido (LIMA, 2019, p. 189).

Com relação às crianças, mormente sob a perspectiva de que se trata de um grupo frágil que deve ser protegido (KOSOVSKI, 2001, p. 2) e considerando que a Constituição da República trouxe a dignidade da pessoa humana como um de seus pilares para evitar injustiças, intolerância e discriminação (BARROSO, 2010, p. 252), há uma maior proteção dos dados pessoais.

Diz-se isso, pois o legislador incluiu no bojo da Lei Geral de Proteção de Dados Pessoais o artigo 14, o qual exige com que o consentimento de utilização de dados de uma criança, considerada aquela pessoa com menos de doze anos de idade (BRASIL, 1990, art. 2º), seja proveniente dos responsáveis.

Lado outro, a rigor, os adolescentes, pessoas na faixa de idade de doze a dezoito anos (BRASIL, 1990, art. 2º), podem, por si só, fornecer seu consentimento. Tratou-se aqui, segundo alguns autores (LIMA, 2019, p. 207), de um lapso normativo que fez com que houvesse um esquecimento quanto à inclusão dos adolescentes no bojo do §1º do artigo 14 da Lei n. 13.709/2018.

Com efeito, é plenamente possível que se tenha o tratamento de dados com base no consentimento do titular e, no caso das crianças, dos seus responsáveis.

1.2.3 *Dos requisitos para o tratamento de dados pessoais de menores*

Não obstante a possibilidade de ter-se um tratamento de dados com base no

consentimento do titular e dos responsáveis por crianças, a lei trouxe outras hipóteses em que, de ofício, poder-se-ia realizar tal ato (LEITE, 2020, p. 43).

Tem-se aqui situações em que são atribuídas obrigações neste sentido ao controlador dos dados, bem como inteligências normativas que possuem o escopo de atingir uma supremacia do interesse público no conceito de, em atendimento a um interesse coletivo, minorar-se um determinado direito individual (MEIRELLES, 2016, p. 113).

Assim, somando-se ao exigível respeito aos princípios estabelecidos na Lei Geral de Proteção de Dados Pessoais e à situação de concordância do detentor, podem ser realizados o tratamento dos dados pessoais para o cumprimento de obrigação legal ou regulatória, execução de políticas públicas, realização de estudos por órgão de pesquisa, existência de necessidade para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, exercício regular de direitos em processo, proteção da vida ou da incolumidade física do titular ou de terceiro, tutela da saúde, atender aos interesses legítimos do controlador ou de terceiro e proteção do crédito.

Acerca da primeira hipótese, qual seja, o cumprimento de obrigação legal ou regulatória, é certo que não se poderia exigir com que um controlador de dados obtivesse uma concordância do titular para cumprir uma obrigação que lhe cabe e, conseguintemente, se sujeitasse a uma sanção por falta de tal aval.

O exemplo claro da inteligência sobre análise é a obrigação de envio, nos termos do artigo 32, da Lei 8.212/91, de informações acerca de obreiros por parte de uma determinada empresa ao Instituto Nacional de Seguridade Nacional (“INSS”). Ou seja, na hipótese de um empregado não concordar em disponibilizar seus dados, a sua empregadora estaria obstada de atender ao comando que lhe é imposto e, por essa razão, seria penalizada (GIMENEZ, 2020).

Cumpre, por oportuno, ressaltar que a Lei Geral de Proteção de Dados Pessoais é clara ao prever que apenas o cumprimento de obrigações estabelecidas em lei ou regulação são capazes de trazer esse tipo de tratamento de dados “automático”. Desse modo, uma obrigação contratual em que se tenha uma necessidade de fornecimento de dados não é apta a ensejar no tratamento que dispensa uma autorização do titular dos dados (LIMA, 2019, p. 179).

No que tange à execução de políticas públicas, importante evidenciar que a Administração Pública poderá, de ofício, realizar um tratamento de dados quando o pano de fundo pretendido for atingir uma conclusão acerca de uma determinada política e sanar eventuais problemáticas relacionadas à saúde, educação, economia e outras questões essenciais (LIMA, 2019, p. 180). Esse ponto, aliás, reforça a ideia de que o Poder Público se submete à Lei Geral de Proteção de Dados Pessoais e que o Estado deve utilizar a grande gama

de dados que possui para concretizar direitos fundamentais (CABRAL, 2020, p. 63).

Os órgãos de pesquisa, os quais, não obstante a existênica de uma discussão para incluir-se empresas privadas cujo escopo é exercer uma atividade acadêmica lucrativa nesse inciso de lei (DALLARI, 2019), podem ser tidos como entidades da Administração Pública, ou pessoas jurídicas privadas sem fins lucrativos que possuem como objeto social a realização de estudos históricos, científicos, tecnológicos ou estatísticos (BRASIL, 2018, art. 5º, XVII), também foram consideradas pelo legislador. Assim, entendeu-se que o resultado de pesquisas, anonimizando-se os dados na exibição do extrato obtido, poderia utilizar o bem jurídico protegido pela Lei Geral de Proteção de Dados.

Além dessas hipóteses, existem situações em que o próprio titular dos dados possui um interesse no tratamento de seus dados como em casos onde a obtenção desse composto de informações é importante para se realizar um contrato. Exemplificando, ao tentar firmar um contrato de financiamento, por certo, o titular dos dados terá mais chances de sucesso se contar com suas informações de crédito junto a instituições financeiras e, conseguintemente, com a transferência de tais dados àquela outra empresa em que se busca o empréstimo (LIMA, 2019, p. 181).

Por essa razão, mesmo porque exige-se um pedido por parte do detentor do dados, não poderia se punir o controlador daqueles bens que realizou o tratamento, sob pena de se incorrer em um verdadeiro *venire contra factum proprium*, ou seja, "dois comportamentos da mesma pessoa, lícitos entre si e diferidos no tempo. O primeiro — o *factum proprium* — é, porém, contrariado pelo segundo" (CORDEIRO, 2013, p. 745).

Comunicando-se com o princípio da inafastabilidade da apreciação pelo Poder Judiciário, bem como com os princípios do contraditório e ampla defesa, o legislador permitiu com que fossem juntados documentos contendo dados pessoais em processos judiciais, administrativos e arbitrais (LIMA, 2019, 181).

A inteligência do artigo 7º, VI, da Lei Geral de Proteção de Dados Pessoais, é importante, como amostra, no momento em que o Fisco necessita ingressar com uma execução fiscal em face de um administrado devedor. Diz-se isso, pois dificilmente se teria um consentimento do devedor para realizar-se o tratamento de dados capaz de substanciar uma cobrança tributária em seu desfavor (FORCENETTE, 2020).

Acerca do tratamento dos dados pessoais em uma situação em que se busca proteger a vida e a incolumidade física do titular dos dados ou de um terceiro, não haveria como se exigir um consentimento. Afinal, a vida é o maior bem jurídico e, por isso, deve ser intensamente protegido, mesmo que isso enseje num decote de outros direitos (SILVA, 2010, p. 202).

Ilustrações de circunstâncias que podem ensejar uma utilização dos dados pessoais sem o consentimento do titular seriam as hipóteses em que, diante de um terremoto, fez-se necessário valer-se da geolocalização contida no aparelho de celular das pessoas que estavam na região atingida no intuito de efetuar-se um resgate (LIMA, 2019, p. 183).

Na mesma toada da proteção à vida e incolumidade física, a norma de proteção de dados pessoais previu uma inexigibilidade de consentimento para os casos que envolvam saúde sem, contudo, abarcar uma situação de perigo de vida (LIMA, 2019, p. 183). A maior problemática aqui se refere ao conceito da expressão "profissionais de saúde" previsto naquela inteligência normativa, pois existe uma ampla gama de trabalhadores envolvidos no setor em questão (médicos, auxiliares, enfermeiros, funcionários administrativos), bem como de terceirizados (SOUZA; LOPES; MELLO, 2018).

Este tipo de tratamento de dados deve ser analisado conjuntamente com a ideia do artigo 11, §4º, da Lei Geral de Proteção de Dados Pessoais (SOUZA; LOPES; MELLO, 2018), de modo que 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 (...).

Somando-se aos demais requisitos imperiosos para um tratamento de dados de ofício, o inciso IX, do artigo 7º, da Lei Geral de Proteção de Dados Pessoais, prevê que o tratamento de dados sem o consentimento expresso do titular pode ocorrer quando existir necessidade atrelada 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" (BRASIL, 2018). Nesse contexto, deve-se caracterizar o interesse legítimo como sendo:

> Outra categoria regulada considerada como uma expressão das interações contextuais ocorridas no ciberespaço é o denominado "interesse legítimo" do controlador dos dados pessoais. Um interesse legítimo pode ser definido como a ampliação da participação que um controlador pode ter no processamento de dados pessoais ou um benefício que o controlador pode obter do processamento. Para ser legítimo, o interesse deve ser suficientemente articulado com as atividades do controlador de modo a permitir que o teste de equilíbrio seja realizado em contraste com os direitos fundamentais do titular dos dados pessoais. Por essa razão, é essencial que se trate de um interesse real e atual, passível de ser exercido em conformidade com a lei, ou seja, algo que corresponda às atividades atuais ou benefícios que são esperados num futuro próximo, o que significa que interesses vagos ou considerados injustificados não serão suficientes.
> Trata-se de uma ferramenta destinada à viabilizar determinadas operações de

> tratamento conduzidas pelo controlador a partir de uma relação intrínseca com suas atividades. Os principais exemplos do uso do interesse legítimo são o marketing direto, as mensagens não comerciais (ex. eleitorais e de caridade), whistleblowing, monitoramento de funcionários para fins de segurança, prevenção à fraude e uso indevido de serviços (SOMBRA, 2019, p. 180).

A maior celeuma no que tange a este dispositivo legal encontra-se na questão do "interesse legítimo de terceiro", porquanto já existem opiniões no sentido de que esta expressão tratou-se, em razão do estabelecido pelo artigo 10, da Lei Geral de Proteção de Dados Pessoais, de um equívoco do legislador. Afinal, aquele artigo 10 faz referência apenas ao interesse do controlador e, de certo modo, é esta a disposição legal que aprofunda a temática aqui contida (LIMA, 2019, p. 185).

Em razão disso, muito embora no regramento europeu tenha se entendido pela possibilidade de inclusão de um terceiro no bojo do tratamento em pauta, há uma sugestão de maior cuidado ao se realizar eventuais tratamentos de dados com base em legítimo interesse de terceiros, em especial até que se tenha uma consolidação jurisprudencial administrativa e judiciária (LIMA, 2019, p. 185).

A última previsão contida na Lei Geral de Proteção de Dados Pessoais acerca do tratamento, de ofício, dos dados pessoais se relaciona à proteção ao crédito. A ideia principal desta disposição legal é no sentido de que as informações acerca da inadimplência e adimplência de um determinado administrado podem ser tratadas para fins de impedir um contumaz descumprimento contratual, principalmente, considerando o Código Consumerista e a Lei do Cadastro Positivo, aqueles que digam respeito à concessão de empréstimos (LIMA, 2019, p. 187).

Por essa razão, o sistema de *score* continuará sendo utilizado em solo brasileiro sem a obrigatoriedade de ter-se um consentimento do titular dos dados.

Dessa forma, são estes os conceitos essenciais para aferir-se o que a Lei Geral de Proteção de Dados visa proteger e, ainda, as hipóteses em que poder-se-á incorrer em atividades que exijam um acesso aos dados pessoais.

1.3 Da transferência de dados

Como mencionado, dentro as possibilidades de tratamento, encontra-se a transferência de dados pessoais. Veja-se que tal atividade, diante da sua ligação com a ideia de vazamento de dados, trará uma clara atuação da Autoridade Nacional de Proteção de Dados e outros órgãos de proteção, de modo que faz-se *mister* evidenciar as circunstâncias em que os

tratadores e controladores dos dados poderão transmiti-los a outrem sem qualquer penalidade.

Nessa senda, demonstra-se interessante trabalhar tanto as especificidades previstas pela legislação para que ocorra uma transferência de dados no âmbito do Poder Público, bem como a pessoas que se situam em outros países.

1.3.1 *Do compartilhamento de dados pela Administração Pública*

Não há como se olvidar que a Administração Pública possui sob o seu domínio uma série de dados pessoais dos administrados. Isso é evidente à medida que são fornecidos aos órgãos públicos dados referentes aos ganhos anuais dos administrados, de tratamentos prestados pelo Sistema Único de Saúde, de questões previdenciárias, imagens, biometria, local de residência e tantos outros (LEVIN, 2020, p. RB-14.1).

Inclusive, a obtenção de tais dados pelo Poder Público acabou por se tornar imprescindível para uma boa atuação governamental. Seria impensável, por exemplo, que fosse prestado um serviço de saúde sem a disponibilização de dados afetos à condição física de um determinado administrado, tampouco seria factível ter-se a prestação de um serviço relacionado à transferência e escrituração de um imóvel sem o devido fornecimento de nomes e documentos das partes envolvidas naqueles atos contratuais e negociais (CARDOSO, 2020).

Nessas conjunturas, é que a Lei Geral de Proteção de Dados Pessoais trouxe, em seu artigo 23, a premissa de que o tratamento de dados pelo Poder Público apenas pode ocorrer quando se tiver uma busca pelo interesse público e para que os entes e entidades públicas cumpram as atribuições legais inerentes à prestação de serviços públicos (BRASIL, 2018). Ou seja, a Administração Pública somente pode tratar os dados de seus administrados com o fito de se alcançar uma regular prestação dos direitos fundamentais e, logicamente, prestigiar os interesses individuais sob uma perspectiva do indivíduo como partícipe da sociedade (BANDEIRA DE MELLO, 2015, p. 66).

E mais, tendo em vista que houve veto ao quanto disposto pelo inciso IV do indigitado artigo em que se tinha uma vedação ao compartilhamento dos dados no âmbito do Poder Público, pode-se concluir, por meio de interpretação *contrario sensu*, que é possível uma transferência, desde que observados os objetivos a serem atingidos, os princípios já evidenciados no bojo do presente trabalho e o dever de indicação de um encarregado pelas operações a serem realizadas, de dados entre órgãos/empresas públicas (FEIGELSON, 2020, p. RB-4.1).

Nesse ponto, não há como se olvidar que traz extrema preocupação a ideia de

privatização de empresas públicas, sobre as quais incidem os requisitos estabelecidos para que seja realizado o tratamento de dados por parte dos órgãos e entes públicos, como os Correios e o Serviço Federal de Processamento de Dados – Serpro, mormente porque, a rigor, os dados pessoais de diversos administrados seriam disponibilizados, sem um prévio consentimento adequado, a uma empresa que seria pertencente à iniciativa privada (FEIGELSON, 2020, p. RB-4.1).

Tal situação, de forma pura e simples, encontraria uma vedação no quanto disposto pelo artigo 26, §1º, da Lei Geral de Proteção de Dados Pessoais, o qual prevê uma série de limitações para que se tenha uma transferência de dados pessoais tratados pela Administração Pública a uma pessoa jurídica de direito privado, sendo certo, ainda, que eventuais convênios que tenham uma atividade com esse escopo deverão ser, nos termos do §2º daquele dispositivo legal, controlados e, em caso de comprovada infração, punidos pela Autoridade Nacional de Proteção de Dados.

Ou seja, ainda que seja possível ocorrer, somente se pode ter um compartilhamento de dados no bojo das pessoas jurídicas que compõem a Administração Pública quando existir o estrito cumprimento e obsrvância aos princípios e requisitos trazidos pela Lei n. 13.709/2018.

1.3.2 *A transferência internacional de dados pessoais*

O artigo 33, da Lei Geral de Proteção de Dados Pessoais, previu os casos em que se pode realizar uma transferência de dados pessoais para países estrangeiros ou organismos internacionais dos quais o Brasil faça parte.

É dizer, assim como ocorreu no Regramento Europeu (“GDPR”), a Lei n. 13.709/2018 trouxe obstáculos para que se tenha um envio de dados pessoais de titulares aqui situados a pessoas jurídicas e entidades encontradas no exterior (IRAMINA, 2019, p. 91).

Tendo em vista a patente ligação entre as hipóteses trazidas no artigo acima citado e a inteligência do artigo 7º, da Lei Geral de Proteção de Dados Pessoais, eis que a transferência internacional de dados pessoais é uma espécie de tratamento (TJUE, 2015), há de se fazer uma breve análise, tendo em vista que a Autoridade Nacional de Proteção de Dados atuará nesse tipo de atividade, acerca das possibilidades legais inerentes à transferência, cujo caráter seja extraterritorial, do bem jurídico aqui em cotejo.

Com esse intuito, há que se colocar que o inciso, I, do artigo 33, da Lei Geral de Proteção de Dados Pessoais, dispõe que pode existir uma transferência internacional de dados pessoais nas hipóteses em que os destinatários desses bens sejam “países ou organismos

internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei". Se está, portanto, diante de situação em que existe um livre fluxo de dados, de modo que, tendo um país/organismo terceiro um nível reconhecidamente adequado, poderá ser realizado o envio dos dados (ARAÚJO, 2017, p. 211).

Essa análise deverá ser feita pela Autoridade Nacional de Proteção de Dados e levará em consideração os requisitos do artigo 34, da Lei Geral de Proteção de Dados Pessoais. Existiu, nesse ponto, uma clara influência do Regulamento Europeu, o que leva a crer que aqueles países tidos como adequados no âmbito de aplicação do GDPR, também, serão vistos como tal no Brasil (CHAVES, 2020, p. 293).

Em seu inciso II, o artigo 33, da Lei Geral de Proteção de Dados Pessoais, prevê que poderá se ter uma transferência de dados pessoais quando "o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei". Esse tipo de prova pode se dar por meio do estabelecimento de cláusulas contratuais específicas ou padrão, normas corporativas globais, selos certificados e códigos de conduta emitidos regularmente.

Trouxe-se, dessa forma, uma exceção ao quanto disposto pelo inciso I, daquela norma legal. Isso porque até mesmo países ou organismos internacionais sem um nível de proteção palpável poderão receber dados pessoais, desde que contem com alguma das circunstâncias estabelecidas nesta inteligência (CAMARINHA; ESPERATO, 2020, p. 122).

Conforme se observa do inciso III, do artigo 33, da Lei Geral de Proteção de Dados Pessoais, permite-se a transferência internacional de dados que tenha como objeto a investigação e persecução de ilícitos. A ideia principal foi ter-se um modo formal de solicitar a outro país uma medida judicial, investigativa ou administrativa que permitisse com que um determinado processo em andamento tivesse o seu devido desfecho.

Justamente por isso, inclusive, é que a operação em questão somente envolve órgãos públicos e, conseguintemente, não pode se ter uma busca por uma investigação privada (TABACH; LINHARES, 2019, p. 147).

O artigo 5º, da Constituição Federal, em seu inciso III, previu que "ninguém será submetido a tortura nem a tratamento desumano ou degradante", de modo que pode-se afirmar que, com base nessa inteligência constitucional, expôs-se uma ideia relacionada à proteção da incolumidade física dos cidadãos, justamente, para fins de evitar um comportamento abusivo de agentes do Poder Público e, também, dos particulares (SARLET; MARINONI; MITIDIERO, 2018, p. 454).

Por conta dessas garantias consitucionais de elevado nível é que o legislador, no inciso

IV, do artigo 33, da Lei Geral de Proteção de Dados Pessoais, entendeu que deveria se permitir uma transferência internacional de dados pessoais nas hipóteses em que houvesse algum risco à vida e à segurança física do titular ou de um terceiro, de modo que, mesmo que o receptor daqueles bens não cumpra com os requisitos de proteção exigidos pela norma ou pelas regulamentações da Autoridade Nacional de Proteção de Dados, a operação poderá ser realizada (CAMARINHA; ESPERATO, 2020, p. 122).

Ou seja, mais uma vez, privilegiou-se, em uma espécie de cotejo de importância, que a saúde e incolumidade física deveria prevalecer sobre os direitos de um titular dos dados pesssoais.

No seu inciso V, o artigo 33, da Lei Geral de Proteção de Dados Pessoais, previu que poder-se-ia realizar uma transferência internacional de dados pessoais quando houver uma autorização da Autoridade Nacional de Proteção de Dados. Por consequência, naquelas hipóteses em que uma determinada questão for submetida ao indigitado órgão, far-se-á uma análise a respeito da possibilidade de que se realize uma transferência internacional de dados a um país que não possui um grau adequado de proteção dos dados pessoais. Inclusive, no regramento europeu, também, existe um dispositivo similar em que, em situações excepcionais, tem-se a possibilidade de recorrer a essa transferência internacional diferenciada (CHAVES, 2019, p. 294).

Obviamente, para fins de não deturpar a pretensão legislativa, tal análise deverá levar em consideração o ponto fulcral da Lei Geral de Proteção de dados e, por essa razão, há que se sopesar se o pleito de transferência de dados formulado contém um justo motivo, sob pena de indenização (CAMARINHA; ESPERATO, 2020, p. 122).

Na hipótese de existir um acordo internacional em que exista um compromisso que depende da transferência internacional de dados pessoais, por certo, conforme o inciso VI, do artigo 33, da Lei Geral de Proteção de Dados Pessoais, poderá ser realizada operação com esses contornos.

A maior diferença entre os incisos III e VI da Lei Geral de Proteção de Dados Pessoais consiste no fato de que, enquanto o primeiro se refere exclusivamente a uma cooperação judiciária entre órgãos públicos, no segundo tem-se uma previsão mais ampla que envolve cooperação administrativa, processual, técnica, financeira e outras (CAMARINHA; ESPERATO, 2020, p. 123). Outrossim, conquanto o inciso III se refira especificamente a órgãos públicos, o inciso VI não faz tal limitação e, portanto, é possível que essa cooperação internacional seja aplicada a entidades pertencentes ao setor privado (TABACH; LINHARES, 2019, p. 149).

Pretendeu-se, desse modo, em atenção ao princípio do *pacta sunt servanda*, fazer com que exista a possibilidade de se dirimir eventuais obstáculos inerentes ao fluxo de dados pessoais com o fito de que o Brasil consiga honrar seus compromissos internacionais (CHAVES, 2019, p. 294).

O inciso VII, do artigo 33, da Lei Geral de Proteção de Dados Pessoais, consigna que é possível realizar-se uma transferência internacional de dados pessoais quando houver uma necessidade "para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei".

Tem-se, assim, dispositivo de norma que aplicável à Administração Pública, justamente porque o artigo 23, I, da Lei, regulamenta o tratamento dos dados pessoais pelas pessoas jurídicas de direito público e, ainda, impõe um dever de publicização, com uma facilidade de acesso, dos atos praticados (TABACH; LINHARES, 2019, p. 149).

Ademais, pode-se afirmar que a transferência internacional aqui em lume deve ocorrer apenas quando houver uma necessidade, é dizer que se trata de operação que deve ocorrer de modo restritivo e limitado e apenas, evidentemente, quando o objetivo perquirido esteja atrelado a um interesse público (CHAVES, 2020, p. 295).

No inciso VIII, do artigo 33, da Lei Geral de Proteção de Dados Pessoais, encontra-se a possibilidade de que, mediante um consentimento específico e com a indicação clara do caráter internacional da operação a ser realizada, os dados de uma pessoa física sejam enviados a países estrangeiros sem um adequado grau de proteção. Isso significa que a informação prévia, específica e com possibilidade real de chamar a atenção dos titulares dos dados da intenção de realizar-se um fluxo transfronteiriço de dados pessoais consiste em condição que, se não for respeitada, gerará a nulidade daquela concordância (BIONI, 2019, p. 202 – 203).

Além disso, o consentimento deve contar com forma escrita e ser livre, de modo que cláusulas com o caráter de *teke it or leave it* não serão tidas como passíveis de ensejar a operação pretendida (CHAVES, 2020, p. 296).

Essa inteligência legal caminhou em sentido diverso do que se observa no regulamento europeu. Isso porque, aquela normativa europeia trouxe que esse aval do titular dos dados somente seria passível de corroborar com uma transferência internacional de dados em casos limitados e específicos, o que não acontece em solo brasileiro (CHAVES, 2020, p. 296).

A última hipótese em que se observa a possibilidade de ter-se um fluxo internacional de dados pessoais a países que não possuem um grau adequado de proteção encontra-se no inciso IX, do artigo 33, da Lei Geral de Proteção de Dados Pessoais, onde se visualiza a premissa de que este tipo de operação pode ocorrer quando o intuito for "atender as hipóteses

previstas nos incisos II, V e VI do art. 7º desta Lei".

O legislador permitiu, assim, com que houvesse uma transferência internacional de dados pessoais quando houvesse tal necessidade para que o controlador de dados cumprisse uma obrigação legal ou regulatória que lhe foi imposta, fosse necessário para a execução do contrato ou a procedimentos preliminares relacionados ao contrato e para exercício regular de direito em processo judicial, administrativo ou arbitral. Incluiu-se, nesse cenário, uma possibilidade de que, mesmo inexistindo uma cooperação internacional nesse sentido, uma determinada empresa tenha os meios necessários a cumprir uma norma de um país estrangeiro que lhe seja aplicável, bem como consiga atender a ordens de processos (judiciais, administrativos e arbitrais) que tramitam no exterior (TANACH; LINHARES, 2019, p. 150).

Importante ressaltar que a ideia aqui disposta consta no *General Data Protection Regulation* e, ali, há uma posição pela interpretação restritiva do termo "necessário", o que permite apontar que conclusão similar deverá ser adotada no Brasil. Dessa forma, deverá haver, por exemplo, uma conexão próxima e profunda entre a transferência de dados buscada e o objeto contratual, de modo que resta, por exemplo, vedada uma transferência internacional de dados embasada em uma decisão empresarial de transferência de seus servidores a um outro país (CHAVES, 2019, p. 296).

Nas mesmas conjunturas, é certo que, ao se pensar na transferência internacional de dados pessoais para fins de permitir um regular andamento processual, engloba-se tanto uma operação que vise a produção de provas quanto a uma efetiva defesa em determinados autos. Todavia, não basta aqui uma alegação de mero "perigo" de processo, sendo certo que o procedimento deve contar com uma materialidade mínima para fins de ser apto a trazer o fluxo de dados aqui em lume (CHAVES, 2019, p. 296).

Sem a observância desses pontos, é indene de dúvidas que a transferência internacional de dados não poderá ser levada a cabo e, caso isso ocorra, deve se uma punição aos responsáveis por tais atos.

1.4 Dos demais aspectos protetivos dos dados pessoais

Como já se ventilou, a proteção dos dados pessoais tem um caráter transversal e, por essa razão, se comunica com diversas áreas do Direito, o que faz com que essa temática seja tutelada por muitos vieses.

Discorrido acerca das conslidações conceituais e operacionais trazidas pela Lei n. 13.709/2018, demonstra-se interessante ilustrar como aquelas ideias se comunicam com

normaivas anteriores, bem como com as outras searas jurídicas.

1.4.1 *Os dados pessoais no âmbito do Direito Bancário*

Nos termos já evidenciados, a Lei Geral de Proteção de Dados Pessoais se somará a outras normas incidentes a outras searas do Direito. Nessa senda, não há como se olvidar que o Direito Bancário, antes mesmo da norma protetiva de dados, já possuía mecanismos para evitar com que as informações de seus usuários fossem difundidas irregularmente.

A propósito, é importante mencionar que a Lei Complementar n. 105/2001 já previa que "as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados" (BRASIL, 2001). Ou seja, o sistema brasileiro em muito se assemelha ao sistema de sigilo bancário dos países da Europa continental, de modo que os bancos não podem divulgar dados econômicos de clientes por uma questão próxima do segredo profissional (ABRÃO, 2018, p. 154).

Apesar disso, conforme dispõe a própria norma em pauta, existirão hipóteses em que o interesse público preponderará, mormente em circunstâncias em que se encontram sob discussão a repressão ao crime organizado e coerção aos delitos relacionados à ordem tributária e previdência social (ABRÃO, 2018, p. 156).

Além da lei em questão, é interessante pontuar que o Banco Central do Brasil, antes mesmo da vigência da Lei Geral de Proteção de Dados Pessoais, trouxe a Resolução n. 4.658/2018 em que se observa a obrigatoriedade de instituições financeiras terem que implementar e manter uma política voltada à segurança cibernética (BANCO CENTRAL DO BRASIL, 2018).

É dizer: a proteção de dados pessoais no âmbito do Direito Financeiro já existe e, conseguintemente, deverá se amoldar, também, ao que dispõe a Lei Geral de Proteção de Dados Pessoais. Nesse contexto, por certo, uma eventual falha de cibersegurança poderá ser apurada tanto no bojo do órgão de proteção de dados quanto pelo órgão que trata das relações entre bancos e clientes.

1.4.2 *Os dados pessoais no âmbito do Direito Concorrencial*

Assim como ocorre nas questões relacionadas aos bancos, é certo que problemáticas que envolvam dados pessoais, também, podem dar ensejo a uma situação concorrencial. Afinal, algumas práticas concorrenciais, como *geo blocking* e *geo locking*, são provenientes

da utilização da geolocalização de um determinado usuário.

Destarte, como já tem sido feito, o Conselho Administrativo de Defesa Econômica continuará sopesando se, por exemplo, o bloqueio de um site a pessoas situadas em uma determinada localização, bem como a aplicação de preços diversos a indivíduos que se encontrem em diferentes cidades, consiste em uma problemática de ordem concorrencial (TERRA; MULHOLLAND, 2019, p. 602). Obviamente, à medida que se tem uma espécie de discriminação, essa mesma questão será cotejada no que tange à utilização dos dados pessoais de forma equivocada, o que pode trazer uma possibilidade de análise por parte de dois órgãos e/ou entidades diversas.

1.4.3 *Os dados pessoais no âmbito do Direito Consumerista*

É indene de questionamento que a temática proteção de dados, considerando a sociedade hiperconectada em que vivemos, tornou-se um crucial ponto de atenção do ponto de vista da proteção do cidadão e do viés consumerista (MENDES, 2014, p. 107 - 116).

Isso porque, a partir dos dados pessoais, poder-se-á ter o que se denomina de *profiling*, ou seja, a formação de um perfil de um determinado indivíduo ou de um grupo de indivíduos com base nas informações por eles disponibilizadas ou colhidas (DONEDA, 2006, p. 173).

Essa prática, notadamente, exige a utilização de fontes atreladas a transações comerciais, perfil em redes sociais, armazenamento de dados de navegação, dentre outros e, ao final, trará, por meio de utilização de algoritmos, uma indicação de comportamento futuro por parte de um usuário (DOHMANN, 2016, p. 536 – 537).

Esse comportamento futuro a ser aferido, por certo poderá se referir a uma análise de consumo, ou seja, um cotejo de dados para quantificar a probabilidade de um cidadão adquirir um determinado produto e, conseguintemente, gerar o direcionamento de publicidades (DONEDA, 2006, p. 173).

Nesse cenário, a utilização de dados nesse contexto poderá consistir em um objeto de monitoramento por parte dos órgãos com o escopo de proteger os consumidores e, simultaneamente, da Autoridade Nacional de Proteção de Dados.

1.4.4 *Os dados pessoais no âmbito do Direito da Saúde*

Além dessa interdisciplinaridade junto aos órgãos de proteção ao consumo, concorrência e das relações bancárias, não há como se olvidar que os dados pessoais terão

forte interação com as normas da Agência Nacional de Saúde Suplementar.

Diz-se isso, pois, desde a Lei n. 9.961/2000, previu-se que a Agência Nacional de Saúde Suplementar detém a competência de estabelecer “as características gerais dos instrumentos contratuais utilizados na atividade das operadoras” e “proceder à integração de informações com os bancos de dados do Sistema Único de Saúde” (BRASIL, 2000). Obviamente, esses pontos, atualmente, deverão ser cotejados por um viés da Lei de Proteção de Dados Pessoais.

Da mesma forma, antes mesmo da lei em questão, aquela autarquia vem evitando uma discriminação de clientes pelas operadoras nos planos de saúde, conforme se nota dos termos do artigo 14, da Lei nº 9.656 e que foi complementada por diversas resoluções (CONFEDERAÇÃO NACIONAL DE SAÚDE, 2021, p. 33).

Nesse cenário, não se tem como olvidar que um malferimento ao bem jurídico aqui em pauta pode trazer uma atuação de duas autoridades, quais sejam, a Autoridade Nacional de Proteção de Dados e a Agência Nacional de Saúde Suplementar.

2 DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Uma das mais importantes figuras trazidas pela Lei Geral de Proteção dos Dados Pessoais, certamente, é a Autoridade Nacional de Proteção de Dados, mormente porque, com o fito de se permitir um sistema eficaz de proteção de dados pessoais, é importante a presença de uma instituição reguladora cujo campo de atenção seja essa temática (PARENTONI, 2019, p. 209).

Em que pese a importância da missão que lhe foi incumbida, não há como se olvidar que a Autoridade Nacional de Proteção de Dados enfrentou percalços relacionados ao seu surgimento. Isso se deve ao fato de que existiu uma grande discussão com relação aos contornos jurídicos que englobariam aquela figura.

Nessas conjunturas, abordar-se-á o processo que ensejou na forma atual da Autoridade Nacional de Proteção de Dados, bem como as funções e atribuições que foram passadas pelo legislador pátrio àquela figura protetiva.

2.1 As discussões legislativas e o surgimento da Autoridade Nacional de Proteção de Dados

Como brevemente colocado, a Autoridade Nacional de Proteção de Dados, em seu formato atual, foi um extrato de longos e profundos debates no bojo dos Poderes Legislativo e Executivo.

Com efeito, até mesmo para se entender de que modo se darão as suas atividades e os limites de suas competências, há que se percorrer, ainda que brevemente, o caminho normativo que criou aquela estrutura em seus contornos presentes.

2.1.1 *O Projeto Original de Lei n. 4.060/2012*

Em uma primeira tentativa de discorrer a respeito da proteção dos dados pessoais dos administrados, o Deputado Milton Monti, em 2012, apresentou o Projeto de Lei n. 4.060.

Aquele Projeto, como se denota de sua própria justificativa, teve como base o V Congresso Brasileiro da Indústria da Comunicação e pretendeu melhor organizar, em especial levando em consideração a grande gama de informações pessoais disponíveis no âmbito da *internet*, a interação dos administrados *online* (BRASIL, 2012).

Nesse intuito, a primeira ideia de norma protetiva de dados foi dividida em três partes e continha vinte e cinco artigos, os quais ventilaram as disposições gerais, princípios, hipóteses

de incidência da norma e os requisitos para que fosse realizado um tratamento de dados.

Apesar de termos, ali, conceitos interessantes, tais como pensamentos iniciais, a ideia de dados sensíveis e uma premissa de autorregulamentação, não houve qualquer menção à criação da Autoridade Nacional de Proteção de Dados Pessoais, ou seja, não se previu, naquele momento, qualquer figura reguladora central que tivesse o intuito de controlar as atividades dos operadores de dados pessoais e, por via de consequência, proteger os titulares daqueles bens.

Nessas conjunturas, apesar dos inegáveis avanços com relação à matéria em lume observados quando do surgimento do primeiro projeto de lei cujo objeto de foco são os dados pessoais, continuou existindo um vácuo legislativo no que tange ao estabelecimento, ao menos de forma unitária, de uma estrutura responsável pela implementação de um efetivo meio e contexto protetivo dos dados pessoais.

Por essa razão, continuaram existindo discussões que, ao final, se desdobraram em novos projetos de leis e em composições provenientes de uma atuação, quase conjunta, dos Poderes Legislativo e Executivo.

2.1.2 *O Projeto de Lei n. 5.276/2016*

Considerando importante a existência de uma figura centralizadora para fins de controlar o uso dos dados pessoais, o Poder Executivo propôs o Projeto de Lei n. 5.276/2016, o qual restou apensado ao Projeto de Lei n. 4.060/2012.

Aquela proposta, notadamente, se mostrou mais robusta que o primeiro texto de lei sobre proteção de dados pessoais; afinal, como se denota de sua breve leitura, ali eram observados cinquenta e seis artigos, que foram embasados em consulta realizada pelo Ministério da Justiça junto à sociedade brasileira (BRASIL, 2016).

Ainda, percebe-se que aquele projeto foi dividido em oito capíulos em que quedaram trazidos os fundamentos, definições e princípios normativos, os requisitos para o tratamento de dados (já com a ideia de consentimento livre e informado), os pressupostos para o tratamento de dados de crianças e adolescentes, os direitos do titular dos dados, os contornos do tratamento de dados pessoais realizado pelo Poder Público, a transferência internacional dos dados, as definições dos agentes de tratamento de dados, as boas práticas com relação à matéria e, por fim, a fiscalização e sanções aplicáveis.

No último ponto, mormente com essa ideia de implementação e fiscalização da lei, é que se previu a criação de um órgão competente para assim agir, bem como de um Conselho

Nacional de Proteção de Dados Pessoais e de Privacidade composto por quinze membros e que deteria uma função consultiva.

Ou seja, o Poder Executivo, por meio do artigo 55 do Projeto de Lei n. 5.276/2016, tentou constituir, sob a forma de um órgão, aquela figura a quem incumbiria dar embasamento a uma política nacional visando a proteção de dados pessoais e privacidade, elaborar relatórios anuais de avaliação da execução daquele plano estabelecido, sugerir ações buscando à proteção dos dados, realizar estudos sobre o tema e disseminar conhecimento acerca da matéria "proteção de dados" (BRASIL, 2016, art. 55).

Visualizou-se, portanto, a ideia de que, para que se atinja a regulamentação pretendida, far-se-ia *mister* uma centralização do controle de eventuais infrações aos dados pessoais para efetivar as funções buscados pelo legislador de "proteger o titular dos dados e, ao mesmo tempo, favorecer a sua utilização dentro de um patamar de segurança, transparência e boa-fé" (BRASIL, 2016).

Em adendo, é importante colocar que o projeto de lei em comento foi alvo de onze propostas de Emendas de Plenário, as quais restaram apresentadas pelos Deputados Weverton Rocha, Jorge Tadeu Mudalen, Leonardo Quintão, Sandro Alex e Paes Landim.

Por meio da Emenda de Plenário n. 1, o Deputado Weverton Rocha pretendeu alterar a redação do *caput* do artigo 50 da normativa, de modo a substituir o termo "poderão", que na visão do parlamentar seria demasiadamente aberto, para "deverão".

Já na Emenda de Plenário n. 2, o referido congressista buscou inserir o inciso V, no artigo 15, do projeto de lei, ou seja, estabelecer que o tratamento de dados pessoais pode ser finalizado por meio de determinação judicial nesse sentido.

A ideia, conforme fundamentação apresentada, seria incluir uma hipótese em que, reconhecida uma atuação abusiva, seja cessada, nos moldes de maior celeridade, a irregularidade.

Na Emenda de Plenário n. 3, o referido deputado intentou suprimir o parágrafo único, do artigo 16, do projeto de lei em comento. Assim, com base na premissa de que estar-se-ia diante de um excesso de poder, a intenção foi impedir que o órgão competente para a análise de eventuais transgressões aos direitos estabelecidos pela norma protetiva dos dados pessoais previsse situações específicas em que restassem conservados os bens jurídicos outrora colhidos.

Por sua vez, em sua Emenda de Plenário n. 4, o Deputado Jorge Mudalen objetivou suprimir as ideias de consentimento informado, visualizada nos artigos 7º, I e 9º, do projeto, e de consentimento informado, expresso e específico com relação ao tratamento de dados

sensíveis.

Discorreu-se, para tanto, que a inteligência de lei proposta estaria em desacordo com a consulta pública efetuada e somente traria maiores dúvidas acerca da temática. Ou seja, pretendeu-se dar um maior valor às reuniões públicas que antecederam na apresentação do projeto de lei proveniente do Poder Executivo.

Na mesma direção de supressão, respectivamente nas Emendas de Plenário n. 5 e 6, o Deputado Leonardo Quintão propôs restringir uma punição solidária de gestores e responsáveis por determinados bancos de dados e o Deputado Sandro Alex almejou que fosse retirada a competência do órgão centralizado de controle de realizar auditorias, estabelecer normas complementares e publicizar suas operações.

Em síntese, tais pretensões foram arrimadas nos pensamentos de que, como o gestor toma decisões que são operacionalizadas por terceiros, não haveria como lhe responsabilizar por eventuais problemáticas exclusivamente atribuíveis àqueles atores externos e de que não poderia se permitir tamanha ingerência nas atividades de tratamento de dados por parte da autoridade controladora.

Finalmente, as Emendas de Plenário enumeradas de 7 a 11, provenientes do Deputado Paes Landim, alteraram algumas inteligências trazidas no Projeto de Lei n. 5.276/2016 quanto ao conceito de uso compartilhado de dados (permitindo-se o compartilhamento de dados pessoais apenas quando houvesse uma delegação legalmente estabelecida).

O conceito supramencionado contempla alguns quesitos:

> a) impõe que o uso compartilhado de dados respeite aos princípios protetivos estabelecidos em norma, inclui a ideia de que é plenamente possível se realizar uma transferência de dados pessoais na hipótese de existir convênio entre entidades privadas;
>
> b) acrescenta a possibilidade de tratamento de dados nos casos em que se pretende a proteção de crédito;
>
> c) inclui a ideia de respeito aos segredos comercial e industrial quando da realização de um determinado tratamento de dados;
>
> d) indica que os dados biométricos somente deverão ser considerados sensíveis quando houver uma clara relação com a raça e etnia do titular dos dados;
>
> e) estabelece que os dados anonimizados passíveis de reversão por meio de procedimento simples, também, serão tidos como dados pessoais.

Percebe-se, portanto, que se está diante de projeto que foi extremamente debatido, seja em razão da discussão realizada junto à sociedade brasileira, travada no seio do Poder

Executivo antes mesmo da apresentação da proposta legal, como dos debates efetivados dentro do Poder Legislativo após a proposição ter sido devidamente protocolada.

2.1.3 *O Projeto de Lei n. 6.291/2016*

Além dos dois Projetos de Lei já mencionados, é imperioso se colocar que, ainda sobre a temática "proteção de dados", foi proposto, pelo Deputado João Derly, o Projeto de Lei n. 6.291/2016.

Naquela proposta legislativa, a qual também restou apensada ao Projeto de Lei n. 4.060/2012, observou-se uma busca pela alteração do Marco Civil da Internet.

Em breve escorço, a intenção do Parlamentar em questão foi, por meio de alterações no Marco Civil da internet, evitar que prestadores de serviços de disponibilização de acesso à rede mundial de computadores compartilhassem os dados pessoais de seus assinantes a empresas terceiras.

Assim, pretendeu-se impedir que os clientes de diversas empresas tivessem os seus dados pessoais comercializados, sem sua autorização, a outras prestadoras de serviços e, consequentemente, tentou-se limitar com que os bens jurídicos aqui em cotejo fossem tratados como uma mera mercadoria. A propósito, confira-se o teor dos artigos que, caso restasse aprovada a proposta apresentada em sua forma original, fariam parte da Lei n. 12.965/2014 (BRASIL, 2016):

> XIV – de não compartilhamento de seus dados pessoais, exceto mediante consentimento livre, inequívoco, informado, expresso e específico pelo titular.
> § 1º Consideram-se dados pessoais qualquer dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa, além de dados relacionados à origem racial ou étnica, às convicções religiosas, às opiniões políticas, à filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, bem como dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos." (NR)
> § 2º Sujeitam-se às punições previstas no art. 12 desta Lei as empresas que violarem o disposto no inciso XIV do art. 7º desta Lei". (NR)

Como se nota, apesar de ser relativamente curta, está-se diante de proposição normativa que versou acerca do direito de não compartilhamento de dados pessoais, de modo a exigir o consentimento do titular para que se tivesse um determinado tratamento.

Além disso, aquele projeto de lei previu sanções, dentro do Marco Civil da Internet, para as situações em que houvesse uma disponibilização de dados pessoais sem a concordância do seu titular.

As pretensões contidas no projeto em evidência, certamente, foram acolhidas na forma final da Lei Geral de Proteção de Dados Pessoais, porquanto, na lei em vigência, se trouxe a exigência de que, dentre outras hipóteses, a realização do tratamento dos dados pessoais de um determinado titular deverá ser precedida do seu consentimento.

2.1.4 *Do Substitutivo do Projeto de Lei n. 4.060/2012*

Diante dos projetos de lei supracitados, bem como considerando as diversas emendas relacionadas ao Projeto de Lei n. 5.276/2016, entendeu a Comissão Especial responsável pela análise do Projeto de Lei n. 4.060/2012, cuja relatoria coube ao Deputado Orlando Silva, que seria a hipótese de apresentar-se um texto de norma substitutivo.

Buscou-se, assim, englobar toda a evolução proveniente dos debates e a unificação de todas as propostas legislativas que tinham como a temática a "proteção de dados", sendo certo que foi este substitutivo que, em agosto de 2018, deu ensejo à Lei n. 13.709/2018.

Como se observa, naquele projeto substitutivo já havia uma previsão no sentido de que seria interessante o estabelecimento de uma figura centralizadora que tivesse como escopo observar o respeito às normas gerais de proteção de dados pessoais e, também, o estabelecimento de regras que trouxessem uma maior segurança aos administrados com relação a essa temática.

Apesar dessa previsão, é certo que a constituição da Autoridade Nacional de Proteção de Dados continuou a gerar discussões que, inclusive, fizeram que o artigo que versava a respeito desse órgão fosse objeto de veto presidencial.

2.1.5 *Do veto presidencial com relação à primeira forma de constituição da Autoridade Nacional de Proteção de Dados*

Aprovado, no teor de seu substitutivo, o Projeto de Lei n. 4.060/12 pelo Congresso Nacional, aquela norma foi levada à sanção presidencial.

Acerca do ponto em que se trouxe a previsão de criação da "Autoridade Nacional de Proteção de Dados (ANPD), integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça" (BRASIL, 2018, art. 55), houve um impasse acerca da existência de um vício de iniciativa.

Isso porque, existiram defensores da tese de que a criação daquela autoridade, pelo fato de trazer novos cargos e órgãos no âmbito da Administração Pública Federal, teria que ser

proveniente do próprio Poder Executivo Federal e, via de consequência, não poderia ser proveniente da Câmara dos Deputados (BRASIL, 2018).

Em outros termos, surgiu uma corrente que ignorou que o Projeto de Lei n. 5.276/2016, proveniente do Executivo e que colaborou para a consolidação do texto substitutivo do Projeto de Lei n. 4.060/12, já previa a criação de órgão público para fiscalizar a observância à Lei Geral de Proteção de Dados (GALVÃO, 2018).

Não obstante as vozes contrárias defendendo que a apresentação de texto normativo do Executivo já contendo a indicação de criação de uma entidade que restaria responsável pela fiscalização de cumprimento das normas de tratamento de dados seria suficientemente apta a ilustrar que a ideia partiu daquele próprio poder, houve veto presidencial da inteligência normativa em cotejo (BRASIL, 2018).

Apesar do referido veto, tendo em vista a importância de se retomar a constituição da Autoridade Nacional de Proteção de Dados, foi apresentada a Medida Provisória n. 869/2018 em que se previa que aquela figura seria um órgão sem aumento de despesa, o que, em 8.7.2019, foi confirmado pela Lei 13.853/2019 (BRASIL, 2019).

Essa criação excepcional, ao que parece, se tratou de uma medida que tinha o escopo de evitar com que, em razão de uma inexistência de uma figura capaz de verificar o cumprimento dos princípios de proteção de dados, fossem obstadas diversas relações comerciais envolvendo o Brasil e países que exigem uma segurança com relação à matéria de proteção de dados. Sobre o tema:

> A fim de evitar barreiras ao comércio internacional que envolvam transferência de dados entre as empresas brasileiras e europeias, posto que a norma europeia (GDPR) dificulta a transferência internacional de dados para dentro do seu limite territorial provenientes de países que não tenham uma lei efetiva sobre o assunto, a aprovação da LGPD ganhou prioridade no Congresso.
> Nesse cenário, houve consenso entre diversos setores de que a lei equilibrava a necessidade de proteção de dados, entendidos como um aspecto da personalidade do indivíduo, com o dinamismo econômico necessário à inovação e à competitividade. Tal consenso encontra fundamento, dentro do panorama econômico atual, especialmente na utilização de dados de pessoas naturais, permitindo uma oferta mais eficiente de produtos e serviços, com benefícios para fornecedores e indivíduos. Por isso, a LGPD congregou o apoio da sociedade civil, consumidores e empresários.
> A regulação da proteção de dados no Brasil requer a conformação de qualquer empresa que realize operação com dados pessoais (entendidos como qualquer informação relacionada a pessoa natural identificada ou identificável), inclusive a coleta, reprodução, transmissão, processamento, arquivamento e a sua eliminação, tanto no ambiente on-line quanto off-line. Desse modo, o setor industrial também deve ser alcançado pela LGPD, a começar pela necessidade de adequação do tratamento das informações pessoais dos seus empregados e colaboradores, dos seus clientes pessoas físicas, da repactuação dos contratos que envolvam a transferência de dados de indivíduos, sem deixar de mencionar a atenção que deverá ser dirigida aos serviços e produtos originados a partir da aplicação da inteligência artificial sobre dados pessoais.

> Pela importância da lei, mas em razão do veto presidencial à Autoridade Nacional de Proteção de Dados (ANPD) e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP), por vício de iniciativa legislativa, o Poder Executivo editou a Medida Provisória 869/2018. A MP formatou o CNPDP e a ANPD, conferindo à autoridade autonomia técnica para desempenhar suas atribuições, como forma de ressaltar a efetividade da norma na proteção de dados, condição essencial para o Brasil buscar o reconhecimento da comunidade internacional. (LIMA; BARBOSA, 2019)

Portanto, hoje, após muita discussão acerca da celeuma apresentada, o que impera é que a Autoridade Nacional de Proteção de Dados, conforme os termos do artigo 55-A, da Lei Geral de Proteção de Dados, se trata de um órgão integrante da Presidência da República cuja constituição se estabeleceu sem aumento de despesa.

2.2 A atuação da Autoridade Nacional de Proteção de Dados

Com a constituição da Autoridade Nacional de Proteção de Dados, fez-se necessário que o legislador estipulasse o âmbito de atuação e objetivo daquela estrutua destinada *prima facie* à proteção dos dados pessoais dos administrados.

Justamente por essa perspectiva é que podem ser vistos diversos prismas contendo previsões de atuação do órgão em questão ao longo da Lei Geral de Proteção de Dados Pessoais.

Além das já vistas hipóteses em que o órgão analisará o direito dos menores e questões inerentes à transferência internacional de dados, terá a Autoridade Nacional de Proteção de Dados diversas outras atribuições que envolvem tanto o exercício de poderes administrativos quanto de outras prerrogativas e que serão elucidadas a seguir.

2.2.1 *Emissão de opiniões técnicas, recomendações, determinações*

Em diversas passagens da Lei Geral de Proteção de Dados Pessoais se consegue visualizar que a Autoridade Nacional de Proteção de Dados detém a competência para emitir opiniões técnicas, recomendações e determinações acerca do tema que regula.

Assim, deu-se àquele órgão a prerrogativa de produzir um ato administrativo de cunho eminentemente jurídico, em especial porque se está diante de uma atuação que se presta "à produção de efeitos jurídicos. São quase sempre emanações de vontade, juízo ou conhecimento do Estado ou de quem lhe faça as vezes, orientadas à obtenção de certos e determinados fins de direito" (GASPARINI, 2008, p. 58-59).

Na maioria das vezes, os atos em comento serão apresentados pela Autoridade

Nacional de Proteção de Dados na forma de um parecer, ou seja, de um documento em que se visualiza uma posição opinativa daquele órgão. Não obstante estar-se diante de um mero parecer, é certo que não se pode ignorar o caráter técnico das conclusões apresentadas pela Autoridade Nacional de Proteção de Dados quando instada.

Afinal, está-se diante de um ato administrativo envolto por uma natureza técnica que o faz sobressair quando cotejado com posições que venham a ser adotadas por outras autoridades. Sobre o que se aduz:

> "Parecer técnico é o que provém de órgão ou agente especializado na matéria, não podendo ser contrariado por leigo ou, mesmo, por superior hierárquico. Nessa modalidade de parecer ou julgamento não prevalece a hierarquia administrativa, pois, não há subordinação no campo da técnica". (MEIRELLES, 2016, p. 220)

Destarte, não obstante não ter um caráter vinculativo propriamente dito, os pareceres e posicionamentos provenientes da Autoridade Nacional de Proteção de Dados só poderão ser desafiados por outro documento com características e pesos similares. É dizer, somente um documento igualmente técnico pode vir a propor um eventual contraponto a uma conclusão daquele órgão sobre uma determinada matéria envolvendo a proteção de dados.

Sequer se poderia entender de forma diversa, porquanto, além de se tratar de uma posição técnica, está-se diante de um ato administrativo que, como tal, possui uma presunção de veracidade e legitimidade que impõe com que quem o desafie traga razões robustas para tanto (CARVALHO FILHO, 2017, p. 110).

São exemplos destes atos envolvendo as conclusões advindas da Autoridade Nacional de Proteção de Dados os modos de atuação trazidos pelos artigos 4º, §3º, 38, *caput*, e 55-J, XI, todos da Lei Geral de Proteção de Dados Pessoais.

A inteligência do artigo 4º, §3º, da Lei Geral de Proteção de Dados é importante, visto que o tratamento de dados será, também, utilizado por atividades que envolvam segurança pública, defesa nacional, segurança do Estado ou investigações no âmbito da Administração Pública.

Ora, faz-se necessário que, diante da enormidade de dados pessoais disponíveis ao Poder Público (como impressões digitais, fotografias, mecanismos de reconhecimento facial, quebra de sigilo bancário), a Autoridade Nacional de Proteção de Dados esboce suas recomendações e posições relacionadas aos mais diversos tratamentos ali realizados, em especial visando estabelecer os contornos das situações excepcionais em que não se aplicará a Lei Geral de Proteção de Dados Pessoais (VAINZOF, 2020, p. 67).

Fazendo-se um paralelo com as agências reguladoras nesse ponto, é certo que a Autoridade Nacional de Proteção de Dados deverá agir com parcimônia no exercício de suas funções, principalmente, nas hipóteses em que estiver sob o seu enfoque de seus pareceres, entes e entidades governamentais.

Afinal, não se pode perder a tecnicidade legalmente exigida por conta de eventuais ingerências políticas. Até por isso, e na busca de uma independência para tratar da temática, há que se manter um certo distanciamento entre o órgão e o Poder Executivo.

Por sua vez, buscando facilitar a sua função fiscalizadora, a Autoridade Nacional de Proteção de Dados pode, nos termos dos artigos 38, *caput*, e 55-J, XI, da Lei Geral de Proteção de Dados Pessoais, determinar que um controlador elabore relatórios atrelados ao impacto e proteção dos dados pessoais.

Esses relatórios consistem em uma descrição dos processos que podem gerar um risco às liberdades civis e direitos fundamentais, bem como como esmiuçar as medidas adotadas para evitar celeumas dessa natureza (LEAL; MELLO, 2020, p. 135).

Nesse contexto, tem-se a possibilidade de que a Autoridade Nacional de Proteção de Dados expeça um ato administrativo que deve ser cumprido pelos administrados. A rigor, portanto, desde que esteja provido de fundamentação e não adentre em segredos comerciais e industriais, não há como os operadores de dados se negarem a dar cumprimento àquela determinação proveniente do órgão protetivo.

A partir disso, evidentemente, a estrutura responsável pela verificação do atendimento aos princípios de proteção de dados pessoais checará o acerto das atividades prestadas por entidades particulares e públicas e, observando uma incongruência, trará sua posição acerca do caso.

2.2.2 *Regulamentação*

Ainda da leitura da Lei Geral de Proteção de Dados Pessoais, depreende-se que caberá à Autoridade Nacional de Proteção de Dados regulamentar diversos pontos encontrados naquela norma. Essa ideia pode ser observada em diversos dispositivos da legislação, em especial nos seus artigos 30, *caput*, 35, *caput*, 40, *caput*, 46, §1º, 53, *caput* e 62, *caput*.

Ou seja, a Autoridade Nacional de Proteção de Dados disporá dos meios necessários para estabelecer requisitos e parâmetros inerentes ao atendimento do escopo de atingir-se uma real e efetiva proteção de dados, bem como para fins de evidenciar os parâmetros para se chegar a uma razoabilidade acerca da aplicação de sanções.

A prerrogativa aqui tratada, é bom que se diga, já passou a ser exercida a partir do momento em que o indigitado órgão editou a Resolução CD/ANPD n. 1/2021.

Naquela resolução, se denota que foram ventilados diversos deveres aos agentes que realizam o tratamento de dados pessoais, como o de fornecer cópias de documentos que possibilitem com que a Autoridade Nacional de Proteção de Dados exerça as suas atribuições, dar ciência àquele órgão a respeito do sistema e contornos dos tratamentos de dados realizados, permitir o acesso da autoridade aos locais e equipamentos utilizados no tratamento de dados, se submeter a auditorias, fazer a guarda das informações dos tratamentos de dados pelo prazo legal e disponibilizar representante, sempre que requisitado, para dar suporte ao órgão governamental.

Ademais, estabeleceu-se a forma de contagem dos prazos para atendimento de eventuais solicitações provenientes do órgão, esclareceu-se o *modus operandi* das operações envolvendo a sua competência fiscalizatória e, também, as premissas iniciais da ideia de cooperação entre as autoridades que tratarão a respeito da matéria de proteção dos dados pessoais (BRASIL, 2021).

Acerca desse tema, merece um maior destaque a figura das empresas públicas, porquanto no próprio bojo do artigo 24, da Lei Geral de Proteção de Dados Pessoais, se visualiza uma especificidade no que tange a essas empresas.

Obviamente, este tipo de pessoa jurídica, a qual atua no âmbito de direito privado e integra a Administração Pública Indireta (OLIVEIRA, 2021, p. 236), mereceu uma maior atenção do legislador, porquanto pode atuar em regime de concorrência ou buscando o atendimento de uma política pública.

De qualquer sorte, é questionável se falar que uma empresa pública, atuando em concorrência, não teria como viés o atendimento de uma política pública. Assim, ainda, que em menor grau, poder-se-ia falar que qualquer empresa pública almeja cumprir um interesse da sociedade, conforme a própria inteligência do artigo 173, da Constitutuição da República (SCHWIND, 2021).

Portanto, algumas empresas públicas poderão se ver obrigadas a atender questionamentos e solicitações provenientes da Autoridade Nacional de Proteção de Dados que sejam direcionadas tanto ao tratamento de dados realizados pelo Poder Público quanto a questões que estejam atreladas a operadores de dados que estejam situados no âmbito da esfera privada.

Na mesma senda, ter-se-á dúvidas com relação à aplicação das penalidades estabelecidas, porquanto, devidamente regulados os processos de fiscalização e sanção

trazidos na Lei Geral de Proteção de Dados Pessoais, é plenamente possível que as penalidades direcionadas ao Poder Público sejam, também, aplicadas em desfavor de empresas públicas, desde que a atuação encontre-se no âmbito da consecução do interesse dos administrados (SCHWIND, 2021).

Colocadas essas nuances, é indubitável que, não obstante já ter iniciado a prerrogativa de regulamentação, a Autoridade Nacional de Proteção de Dados deverá seguir trazendo maiores normativas capazes de explicitar os moldes em que se dará a busca pela proteção dos dados pessoais.

2.2.3 *Fiscalização e punição*

Além das atribuições acima relatadas, é possível extrair da Lei Geral de Proteção de Dados Pessoais que a Autoridade Nacional terá os deveres de fiscalizar o cumprimento da norma, bem como, visualizando uma infração, punir o agente em desacordo com as previsões legais.

E sequer poderia ser diferente, eis que um órgão com a pretensão de controlar o bom uso dos dados pessoais deve ter um papel fiscalizador, o qual pode ser exemplificado por meio dos artigos 10, § 3º, 20, §2º, 32, 35, *caput* e incisos e 38, *caput* e incisos, todos da normativa supracitada. Ou seja, nota-se que o órgão em questão detém uma competência para exigir a apresentação de Relatório de Impacto à Proteção de Dados Pessoais e, conseguintemente, valer-se de tal documentação para fins de observar o acerto das medidas tomadas pelo controlador dos dados para, exemplificadamente, evitar um vazamento de dados (LIMA, 2020, p. 196).

Do mesmo modo, a Autoridade Nacional pode realizar uma auditoria naquelas hipóteses em que um controlador dos dados se negar a atender solicitação de revisão de decisões tomadas por meio de tratamento automatizado de dados pessoais.

Nesse contexto, o órgão verificará a higidez do motivo apresentado para não disponibilizar aquelas informações, mormente porque a tecnologia deve atender ao que a norma preconiza (SELBST; POWLES, 2017). Ademais, por certo, todos os pontos constantes no artigo 55-J, da Lei Geral de Proteção de Dados Pessoais exigirão que a Autoridade Nacional atue de modo preventivo na busca de impedir que infrações sejam suportadas pelos administrados.

Ora, se em uma fiscalização se observar um não atendimento ao que consta na norma, a Autoridade Nacional poderá, conforme o artigo 55-K da lei em comento, aplicar uma

penalidade. Essas penalidades, como já brevemente colocado, tiveram o seu processo devidamente regulado por meio da Resolução n. CD/ANPD 1/2021, sendo certo que, ali, já até se visualiza uma diferenciação entre a ideia de sanção e orientação, acerca da determinação do cumprimento da punição estabelecida em primeira instância e com relação à possibilidade de revisão da decisão punitiva por parte do órgão protetivo (BRASIL, 2021).

2.3 O caráter das atuações ventiladas e da possibilidade de sua delegação a terceiros

Apresentadas as atuações trazidas pela normativa à Autoridade Nacional de Proteção de Dados, há que se apontar, até mesmo buscando visualizar-se a possibilidade de se ter uma delegação, no que consistem aquelas atribuições. Essa indicação das naturezas das atividades exercidas será esmiuçada por meio das colocações a seguir apresentadas.

2.3.1 *Do caráter de Poder Administrativo Regulamentar*

Como devidamente trabalhado, a Lei Geral de Proteção de Dados Pessoais previu que a Autoridade Nacional de Proteção de Dados teria a competência para emitir opiniões técnicas, recomendações, determinações, editar regulamentos, fiscalizar e punir.

Com relação ao ato de editar regulamentos, faz-se *mister* consignar que, ao que tudo indica, concedeu-se ao órgão em comento um Poder Regulamentar, pois se permitiu que a figura em pauta, sem inovar o ordenamento jurídico e apenas de forma complementar, atue com a finalidade de estabelecer regras para que seja cumprida a vontade do legislador (MEDAUAR, 2018, p. 109).

Apesar dessa premissa, não há como se olvidar, nos termos do artigo 55-A da Lei Geral de Proteção de Dados Pessoais, que a Autoridade Nacional de Proteção de Dados, ao menos por enquanto, é um órgão do Poder Executivo Federal.

Essa circunstância, certamente, exige com que se aborde se houve um malferimento ao quanto disposto pelo artigo 84, IV, da Constituição da República, no qual se tem que o Poder Regulamentar relacionado à expedição de decretos é privativo do Chefe do Poder Executivo Federal. A propósito:

> A competência privativa é aquela que dá exclusividade ao seu titular, não a compartilhando com mais nenhum Poder Político, sendo pois diferente da competência concorrente ou, também, da comum. Existem matérias típicas do Executivo, como as relativas a relações internacionais e aos casos de guerra e paz. Por outro lado, existem atribuições de natureza legislativa, como a iniciativa de leis

> e as medidas provisórias. Outras, ainda que de natureza administrativa, como nomeação para cargos, foram para o Poder Judiciário ou o Tribunal de Contas da União, órgão auxiliar do Legislativo. Na verdade, os incisos do art. 84 da CF, indicam que o sistema de separação de poderes, na verdade, é um sistema de compartilhamento de competência entre os Poderes Políticos.
> (...)
> Dispõe o inciso IV do art. 84 da CF sobre a competência do Presidente da República para sancionar, promulgar e fazer publicar as leis, assim como expedir decretos e regulamentos para a fiel execução das mesmas. O sistema constitucional de controle entre os Poderes Políticos, checks and balances, ou de freios e contrapesos, está demonstrado na competência do Legislativo para sustar atos normativos do Poder Executivo que exorbitem o poder regulamentar ou os limites de delegação legislativa, como indica o inciso V do art. 49. A lei tem caráter geral e abstrato, quase sempre precisando de um decreto que a regulamente. Cabe ao Presidente da República expedir decretos e regulamentos para a fiel execução das leis, conforme o inciso IV do art. 84. (COSTA, 2012, p. 301)

Assim, em que pese, a princípio, se ter uma ideia de que existiu uma inconstitucionalidade ao se atribuir à Autoridade Nacional de Proteção de Dados o referido poder, devem ser feitas algumas considerações acerca do tema. É que, apesar da premissa de privatividade contida no artigo 84, IV, da Constituição da República, não há como se olvidar que se está diante de matéria completamente técnica e que, corolário lógico, não necessariamente será devidamente compreendida pelo Presidente da República.

Em outros termos, parece que a mitigação dessa ideia de exclusividade relacionada à edição de decretos restou, mais uma vez, esboçada no arcabouço jurídico pátrio, de modo a se entender que, naquelas hipóteses muito específicas e técnicas, poder-se-ia realizar uma delegação do Poder Regulamentar dentro da própria Administração Pública (ARAGÃO, 2004, p. 406), o que é a exata moldagem do caso em análise.

Ademais, é importante destacar que o §1º, do artigo 55-A, da Lei Geral de Proteção de Dados Pessoais, já indicou que a Autoridade Nacional de Proteção de Dados terá contornos de uma autarquia especial. Nessa linha de raciocínio, é quase impossível não se atribuir, mesmo que indiretamente, as características de autarquia ao órgão aqui tratado.

Isso faz com que, ainda que se trate de uma passagem de poder a um dos "círculos de atribuições, os feixes individuais de poderes funcionais repartidos no interior da personalidade estatal e expressados através dos agentes neles providos" (MELLO, 1975, p. 69), não exista uma irregularidade na atuação em questão.

Traz-se essa colocação, porquanto, após o surgimento das agências reguladoras, passou-se a entender que é "natural e jurídico que a competência normativa atribuída às agências regulatórias pelas respectivas leis orgânicas traduz um poder regulamentar de 2º grau, que há de ser compatibilizado com o sistema hierárquico de normas legais e infralegais presidido pela constituição rígida" (CASTRO, 2005, p. 65 – 70). Ou seja, não obstante possa

se ter uma primeva ideia de equívoco legislativo em cotejo com o texto constitucional, existem plenas possibilidades para que a delegação de Poder Regulamentar ocorra *in casu*.

Nas mesmas conjunturas, ainda aproximando-se o Poder Regulamentar passado à Autoridade Nacional de Proteção de Dados do que se observa nas autarquias, é imperioso que se coloque a teoria da captura no âmbito do órgão protetivo de dados.

Ora, se a pretensão é buscar uma função reguladora e sendo certo que "no domínio da função reguladora devem predominar as escolhas técnicas, preservadas das disputas partidárias e das complexidades dos debates congressuais, mais apropriados às escolhas político-administrativas" (BARROSO, 2017, p. 285-286), é importantíssimo que a Autoridade Nacional de Proteção de Dados pondere os interesses das pessoas reguladas, dos detentores dos dados pessoais e, ainda, os interesses políticos governamentais.

Bem verdade, portanto, apesar de ainda não existir em âmbito brasileiro uma lei prevendo uma estruturação única de figuras que possuam o espeque regulador (JUSTEN FILHO, 2002, p. 588), jamais poder-se-ia deixar de lado o interesse público em eventual divergência de interesses. Ou seja, há que se evitar:

> A doutrina cunhou a expressão 'captura' para indicar a situação em que a agência se transforma em via de proteção e benefício para setores empresariais regulados. A captura configura quando a agência perde a condição de autoridade comprometida com a realização do interesse coletivo e passa a produzir atos destinados a legitimar a realização dos interesses egoísticos de um, alguns ou todos os segmentos empresariais regulados. A captura da agência se configura, então, como mais uma faceta do fenômeno de distorção de finalidades dos setores burocráticos estatais. (JUSTEN FILHO, 2002, p. 369-370)

Exposto de outra maneira, é necessário que a Autoridade Nacional de Proteção de Dados ignore o poderio de alguns *players* do mercado, como Google e Facebook, para exercitar as funções que, legalmente, lhe foram direcionadas.

Certamente, haverá uma grande pressão sobre o órgão, contudo, a própria lei estabelece com exatidão a autonomia da Autoridade Nacional de Proteção de Dados, o que faz com que se permita criar, ao menos na teoria, uma resistência com relação às pressões externas advindas de terceiros.

2.3.2 *Do caráter de Poder de Polícia*

Além do Poder Regulamentar, ao indicar que a Autoridade Nacional de Proteção de Dados Pessoais teria a ingerência para emitir pareceres, fiscalizar e punir, é certo que deu o

legislador pátrio o Poder de Polícia àquele órgão de proteção de dados.

E essa perspectiva é de fácil observância, mormente porque o poder aqui analisado se configura como sendo "a atividade do Estado consistente em limitar o exercício dos direitos individuais em benefício do interesse público" (DI PIETRO, 2020, p. 323).

Até por isso, inclusive, é que se costuma salientar que o Poder de Polícia se divide em algumas fases, quais sejam: (i) ordem de polícia, ou seja, existir uma norma que limite uma liberdade de um administrado; (ii) consentimento de polícia, que significa uma autorização ou concessão para exercício de um direito; (iii) fiscalização administrativa, a qual está atrelada ao controle do cumprimento das normas; e (iv) a sanção de polícia, onde são aplicadas as penalidades apontadas em lei aos infratores que restarem caracterizados (MOREIRA NETO, 2014, p. 534).

Evidentemente, apesar das fases acima, exige-se que o Estado adote ações concretas para perfectibilizar o poder que a ele foi atribuído; eis que se poderia dizer que se está defronte a um aspecto macro de atuação e, consequentemente, de uma mera estratégia que, por si só, não é capaz de produzir efeitos (PEREIRA, 2013, p. 84).

Destarte, como defende Marrara (2014, p. 569-570), os prismas do Poder de Polícia dependem de uma atuação para que sejam expressados, tais quais: (i) atos normativos (como, por exemplo, normativas que trazem os requisitos para a concessão de autorizações e licenças); (ii) atos administrativos que modificam, condicionam ou impedem com que direitos sejam exercidos; (iii) atos técnicos e opinativos; (iv) atos de execução, como o recolhimento de documentos, destruição de objetos advindos de ilícitos; e (v) acordos firmados pela Administração Pública.

Com base em tais ensinamentos, é inquestionável que a Autoridade Nacional de Proteção de Dados poderá atuar arrimada no Poder de Polícia, em especial ao se observar diversos artigos da Lei Geral de Proteção de Dados (especialmente as disposições contidas nos incisos e *caputs* dos artigos 35, 55-J e 55-K, daquela lei).

Outrossim, importa mencionar que a transferência internacional de dados pessoais merece aqui uma melhor atenção. Afinal, o estabelecimento do conteúdo de cláusulas contratuais padrão, conforme o indicativo do artigo 35 da Lei Geral de Proteção de Dados Pessoais, se trata de uma atribuição dada pelo Legislador à Autoridade Nacional de Proteção de Dados e que, por envolver um ato voltado à concessão de uma espécie de "autorização" para realização de uma transferência de dados, se trata de uma das facetas do Poder de Polícia, mormente a fase de consentimento de polícia.

Ocorre, no entento, que existe naquele mesmo artigo a possibilidade de realizar-se uma

delegação a “organismos de certificação”, de modo que, a princípio, ter-se-ia como hígido o repasse da faceta de Poder de Polícia sobre análise a entidades que se encontram no plano privado.

A delegação aqui em cotejo restou, recentemente, analisada pelo Supremo Tribunal Federal que, partindo da perspectiva dos ciclos de polícia na hipótese do julgamento do Recurso Extraordinário n. 633.782, entendeu ser plenamente possível o repasse dos aspectos de consentimento e fiscalização a entes privados. A propósito:

> A *vexata quaestio* ora submetida à apreciação deste Plenário gravita em torno de um dos temas mais sensíveis do Direito Administrativo contemporâneo, objeto de ampla reflexão doutrinária, acadêmica e jurisprudencial. Isso porque a indispensável definição acerca da possibilidade do exercício do poder de polícia administrativa por pessoas jurídicas de direito privado integrantes da Administração Pública indireta impõe a análise detida das mais variadas visões existentes na doutrina e prática jurídica brasileira.
> (...)
> A doutrina, por sua vez, criou a teoria do ciclo de polícia, que se desenvolve em quatro fases, cada uma correspondendo a um modo de atuação da Administração: a ordem de polícia, o consentimento de polícia, a fiscalização de polícia e a sanção de polícia.
> (...)
> Por fim, cumpre ressaltar a única fase do ciclo de polícia que, por sua natureza, é absolutamente indelegável Por fim, cumpre ressaltar a única fase do ciclo de polícia que, por sua natureza, é absolutamente indelegável: a ordem de polícia: a ordem de polícia, ou seja, a, ou seja, a função legislativa. Os atos de consentimento, de fiscalização e de aplicação de sanções podem ser delegados a estatais que, à luz do entendimento desta Corte, possam ter um regime jurídico próximo daquele aplicável à Fazenda Pública. função legislativa. Os atos de consentimento, de fiscalização e de aplicação de sanções podem ser delegados a estatais que, à luz do entendimento desta Corte, possam ter um regime jurídico próximo daquele aplicável à Fazenda Pública. (BRASIL, 2020)

Portanto, superou-se a posição que outrora era esboçada pela Corte Suprema quando do julgamento da Ação Direta de Inconstitucionalidade n. 1717. Anteriormente, o que se tinha era a conclusão pela indelegabilidade plena do Poder de Polícia, porém, nos dias atuais, impera a posição de que apenas as facetas do Poder de Polícia da ordem de polícia, a qual é extritamente atrelada ao Poder Legislativo no estabelecimento de limites à atuação dos administrados, e da sanção de polícia, consistente na punição por parte do Poder Público, devem permanecer no âmbito da Administração Pública e não poderiam ser delegadas.

Por essas razões, estando-se diante de uma mera delegação de consentimento de autorização para uma transferência internacional de dados, não há como se olvidar do acerto do legislativo do ponto de vista constitucional afeto à delegação de poderes administrativos (especificamente, o Poder de Polícia).

2.3.3 *Da ideia de "third party verification"*

Da mesma forma, poderia se considerar que a delegação da atribuição relacionada à verificação das cláusulas contratuais padrões estabelecidas para realização de uma transferência internacional de dados pessoais se aproximaria muito da figura da *third party verification*. Essa ideia se atrela ao pensamento de que, em especial no §3º, do artigo 35, da Lei Geral de Proteção de Dados Pessoais, existiu uma opção técnica visando se impedir a repetição de manchetes jornalísticas que, ao fim e ao cabo, tenham como pano de fundo uma falha de cunho fiscalizatório (sendo um exemplo disso, no Brasil, uma falha de verificação que culminou no desmoronamento da barragem de Mariana, Minas Gerais).

Bem verdade, as dimensões em que se encontram a proteção de dados pessoais, até mesmo em razão da rede mundial de computadores e sua profundidade, são enormes e, por esse motivo, dificilmente o Estado terá verba suficiente para efetivar e implementar o que restou estabelecido em norma (por exemplo, faltarão pessoas suficientemente aptas à proceder com a verificação das mais diversas operações internacionais envolvendo a transferências de dados).

Assim, é que, em muitos casos, se demonstra até mesmo mais eficaz que sejam repassadas a um terceiro, em uma perspectiva de somar forças, determinadas obrigações, impondo-se que, em algumas esferas de atuação, o Poder Público tenha uma confiança em um particular para que atue em seu lugar e, em seguida, fiscalize o trabalho feito por sua entidade auxiliadora (MCALLISTER, 2012, p. 41).

Logicamente, esse *modus operandi* possui pontos positivos e negativos. Cabe citar, a título de ponto positivo, a possibilidade de se ter uma maior aproximação entre as unidades certificadoras e aquelas empresas reguladas, mormente porque, diante da incapacidade de aplicação de sanção daqueles terceiros, existe um maior espaço para o diálogo e troca de informações (MCALLISTER, 2012, p. 14).

Essa aproximação traz consigo um maior aprendizado e permite uma evolução mais orgânica entre o órgão de proteção e as empresas que são reguladas por ele. Diz-se isso, pois, a princípio, os terceiros responsáveis pela certificação mencionada em lei estariam em um pé de igualdade quando comparados com as entidades privadas que regulam, o que, em razão das prerrogativas exercidas pela Administração Pública, não ocorreria com um exercício da atribuição sendo realizado diretamente pela Autoridade Nacional de Proteção de Dados.

Lado outro, já tendo em vista os perigos da regulação por terceiros, poder-se-ia mencionar que, enquanto as unidades certificadoras e entidades privados evoluem cada vez

mais, a Administração Pública, ao terceirizar essa função, deixaria de ter um crescimento em uma determinada área da matéria "proteção de dados" (MCALLISTER, 2012, p. 23).

Nesse cenário, será necessário exercer, em muitos mais hipóteses, as premissas contidas na Resolução CD/ANPD Nº 1/2021, primordialmente aquelas que trazem como um dever das empresas reguladas disponibilizar relatórios e abrir as características dos tratmentos de dados realizados por meio da disponibilização de pessoa capacitada. Com base nessas colocações, em que pese estar-se diante de um modelo realmente inovador no Brasil, tem-se que é imperioso que o Poder Público permaneça, ao menos de alguma forma, atuando no intuito de verificar a transferência internacional de dados lastreada em cláusulas contratuais-padrão (mesmo que indiretamente).

2.3.4 *Da ideia de autorregulação regulada*

Em adendo aos Poderes já mencionados, há que se colocar que a Lei Geral de Proteção de Dados Pessoais, em seus artigos 46 e 50, trouxe uma perspectiva de autorregulação regulada. É que, conforme se depreende daquele dispositivo legal, serão trazidos pela Autoridade Nacional de Proteção de Dados apenas os padrões técnicos mínimos no que tange à adoção de medidas de segurança pelos operadores de dados (PEREIRA; ALVIM, 2020).

Com efeito, caberá aos próprios operadores de dados trazerem normas internas para efetivarem a segurança no tratamento de dados, sendo certo que se está diante de uma verdadeira hipótese em que se tem uma "forma de regulação estatal do mundo empresarial, subordinada a fins ou interesses públicos pré-determinados pelo Estado (...) no interesse em reorientar sua atuação por um intervencionismo à distância" (COCA VILA, 2013, p. 51).

Ou seja, trouxe-se uma liberdade para que as entidades que trabalhem com o manuseio dos dados pessoais amoldem às suas atividades a segurança exigida pelo legislador pátrio, de modo a se tornar clara a existência de uma repartição da competência normativa para fins de estabelecimento de normas gerais e de normas específicas (PEREIRA; ALVIM, 2020).

Aqui, é importante consignar que se exige uma atuação conjunta e que não destoe das premissas trazidas pelo legislador, mesmo porque, repise-se, o Estado continuará realizando, mesmo que de forma mais afastada, o controle acerca das medidas tomadas pelos tratadores de dados pessoais com o fito de evitarem vazamentos e outras questões problemáticas.

2.3.5 *Das ideias de "hard law e soft law"*

A título de somatório com relação às outras características da atuação da Autoridade Nacional de Proteção de Dados previstas na Lei Geral de Proteção de Dados Pessoais, é importante destacar que a própria legislação protetiva de dados prevê hipóteses em que serão estabelecidos acordos internacionais para tratar da temática.

Essa premissa pode ser extraída da inteligência do inciso VI, do artigo 33, da lei em tela; ou seja, desde logo, permitiu-se com que sejam realizadas transferências internacionais de dados pessoais que tenham como pano de fundo uma norma proveniente do direito externo capaz de produzir efeitos internamente (SHAFFER; POLLACK, 2011, p. 713).

Por consequência, se tem como cristalino que a cooperação internacional é plenamente capaz de inovar nas políticas internas de transferência transfronteiriça de dados pessoais, sendo certo que impor-se-á uma atuação orgânica da Lei Geral de Proteção de Dados Pessoais e eventuais acordos internacionais.

Da mesma forma, é notório que existe espaço para que a proteção de dados, ainda que por meio de discussões não vinculativas, não se mantenha estanque. Em outros termos, é claro que a Autoridade Nacional de Proteção de Dados poderá – se utilizando de normas e princípios gerais que não consistam em regras obrigatórias, ou seja, de *soft law* (SHELTON, 2010, p. 160) – rever seu posicionamento.

Na mesma toada, é certo que, em algumas hipóteses, normativas específicas de um determinado setor, não obstante serem desprovidas de caráter vinculante, poderão agregar com relação ao intuito de proteção de dados pessoais.

A título exemplificativo, as especificações direcionadas ao campo do sigilo médico se demonstram mais completas do que os princípios gerais da Lei Geral de Proteção de Dados Pessoais (MENEZES, 2020), de modo que podem, ainda que sob a premissa de um *soft law*, lastrear a atuação da Autoridade Nacional de Proteção de Dados.

Assim, ao menos em certa medida, evita-se que exista um engessamento das normas protetivas nacionais com relação a entes estrangeiros e até mesmo entidades internas, de modo a se permitir uma constante evolução em matéria de proteção de dados. Nesse contexto, não há como se olvidar que a Lei Geral de Proteção de Dados Pessoais permite com que o órgão protetivo busque inspirações internas e externas para otimizar e atingir os seus objetivos pretendidos.

2.3.6 *As premissas de coordenação e cooperação*

Além de todos esses pontos, é fácil perceber que a Lei Geral de Proteção de Dados

Pessoais previu em seu bojo as ideias de coordenação e de cooperação. Isso, aliás, é extraído do teor dos artigos 55-J, XX e 55-K, *caput* e parágrafo único, daquela legislação.

Assim, o legislador, já prevendo uma possibilidade de atuação conflitante entre dois atores internacionais e outras instituições nacionais, estabeleceu que aquele órgão deverá, por meio de um papel preponderante, atuar de forma harmoniosa com outras entidades que regulem a matéria sob debate.

Portanto, apesar de ser inequívoco que caberá à Autoridade Nacional uma posição de destaque, exige-se aqui um consenso com relação ao entendimento proveniente daquele órgão juntamente com aqueles advindos de pessoas situadas no exterior, órgãos integrantes do Sistema Nacional de Defesa do Consumidor, o Ministério Público, o Poder Judiciário, agências reguladoras e outros legitimados (MONTEIRO; CRUZ, 2021, p. RB-8.11).

Buscou o legislador, simultaneamente, evitar com que existissem atritos institucionais envolvendo a matéria proteção de dados pessoais e fazer com que surgisse uma perspectiva de colaboração, e não colisão, entre entidades que versam acerca daquele tema, o que, certamente, fará com que se estabeleça uma maior segurança jurídica no cenário nacional (ZANATTA; SIMÃO; OMS, 2018, p.7)

Por assim dizer, até mesmo considerando a inteligência do artigo 18, §8º, da Lei Geral de Proteção de Dados Pessoais, caberá ao administrado que tiver seus direitos violados estudar se entende mais produtivo apresentar suas reclamações à Autoridade Nacional de Proteção de Dados ou, por exemplo, alguma outra entidade (como o Procon).

Certamente, apesar de se ter esses princípios na norma, é complexo se fazer com que a última palavra com relação às matérias que envolvam dados pessoais seja da Autoridade Nacional de Proteção de Dados quando existem diversos outros órgãos independentes que possam tratar da mesma celeuma apresentada.

3 DO POSSÍVEL CHOQUE NA DEFESA DOS DADOS PESSOAIS

Elucidados os contornos da atividade repassada pelo legislador pátrio à Autoridade Nacional de Proteção de Dados, há que se conceituar as ideia de conflito de atribuições e de conflito de competência, bem como esclarecer de que modo poderia ocorrer essa circunstância no caso da proteção de dados pessoais.

Isso porque, como é de conhecimento, o ordenamento jurídico pátrio não admite o *bis idem*.

Assim, ao longo do presente capítulo, serão trabalhados conceitos relacionados às figuras aqui em menção, mormente para que, ao final, se consiga analisar as medidas para evitar problemáticas de competência.

3.1 Do princípio do *ne bis in idem*

A jurisprudência pátria estabeleceu em seu bojo a conclusão de que o *bis in idem* não pode ser aceito em território nacional, de modo que, por essa razão, trouxe-se uma limitação ao poder Estatal de punição. É dizer, considerando que o *ius puniende* previsto em norma, que deve ser suficiente para contrapor a ilegalidade a que combate, que não haveria como se elastecer a pretensão de correção do Estado (GARCÍA ALBEIRO, 1995, p. 79)

O raciocínio lógico para tanto consiste na perspectiva de que, na busca de se atender direitos fundamentais previstos na Constituição da República e em respeito a uma premissa de equidade, não parece justo e sequer coerente que um determinado sujeito receba duas penalizações por uma mesma conduta ilegal. Ou seja, como bem colocado por Muñoz Clares (2006, p. 259), assim como "o toque da tecla de um piano dá lugar a um único som, um só fato deve dar lugar a uma só consequência jurídica estabelecida pelo direito sancionador".

No mesmo sentido, é certo que essa impossibilidade de punição traz consigo uma segurança jurídica, mormente porque trouxe-se aqui uma

> dupla funcionalidade substantiva e processual do *non bis in idem* (...) nascido com um instituto processual vinculado à idéia de coisa julgada (...) o que enfatiza a idéia de segurança jurídica, este princípio evolui até o terreno muito mais substancial e consistente da proibição de inflição de duplo castigo a um mesmo sujeito por idênticos fatos (...) (QUERALT, 1992, p. 10).

Contudo, especialmente para se entender como se deu a construção do instituto, há que se rememorar, ainda que brevemente, os contornos em que se deram o surgimento do *ne bis in idem* e o seu desenvolvimento ao longo dos anos, bem como a forma em que essa concepção

se lastreou para as mais diversas searas do Direito.

3.1.1 *Do contexto histórico do princípio do "ne bis in idem"*

Como qualquer instituto que já seja observado por vários anos, é extremamente complexo saber-se com exatidão a data de surgimento do princípio do *ne bis in idem*.

Apesar dessas dificuldades, no direito romano já se poderia ver uma forma inicial do princípio em questão, seja quando da vigência da Lei das Doze Tábuas (ROCCO, 1932, p. 44), no Digesto de Justiniano (LEÓN VILLALBA, 1998, p. 34) ou quando observado o fenômeno da consunção (RAMOS, 2009, p. 56).

Como as primeiras manifestações do *ne bis in idem* eram interligadas a um contexto de não se poder buscar um mesmo direito mais de uma vez, é possível dizer que, em um momento inicial, este instituto se relacionava mais especificamente com questões civilistas, tal qual uma ideia de coisa julgada (COSTA, 2012, p. 58).

Apenas mais posteriormente é que o cânone aqui tratado foi elastecido para a seara do Direito Penal, sendo certo que se passou a impedir com que diversas acusações, que tivessem como base o mesmo delito, fossem direcionadas a um mesmo sujeito (SANZ MORÁN, 1986, p. 51).

Em razão de os países latino-americanos, não obstante as modificações que aquele *codex* sofreu ao ser incorporado por países da Europa Ocidental, terem uma forte influência do Direito Romano (AZEVEDO, 2000, p. 205), houve uma incorporação do instituto no ordenamento jurídico brasileiro. Inclusive, como prova dessa importação ocorrida, não é raro se fazer uma interligação entre o princípio do *ne bis in idem* com a coisa julgada no Brasil, tanto o é que o próprio Supremo Tribunal o fez quando do julgamento da Reclamação 41.557/SP (BRASIL, 2020).

Além dessa adoção interna por parte de Estados do indigitado princípio, é certo que existiu uma compreensão internacional relacionada ao tema (SABOYA, 2014, p. 39). Diz-se isso, pois nos Tribunais internacionais também impera a perspectiva de que há que se trazer uma segurança jurídica com relação à coisa julgada, ou seja, nesse prisma o *ne bis in idem* ainda se encontra muito atrelado a uma noção de decisão imutável.

É por essa razão, aliás, que o Supremo Tribunal Federal, quando da análise do HC 171.718/SP, consignou que, por força dos artigos 14.7 do Pacto Internacional sobre Direitos Civis e Políticos e 8.4 da Convenção Americana de Direitos Humanos, não haveria como se ter uma persecução penal no Brasil quando já existiu uma ação proposta no exterior com base

nos mesmos fatos. Confira-se:

> Desse modo, o que se deve debater diz respeito ao conteúdo da proibição de dupla persecução e seus impactos no processo penal brasileiro. Basicamente, o problema a que se pretende responder é: o direito de não ser processado duplamente por fatos já julgados se aplica também em âmbito internacional? Desse modo, o que se deve debater diz respeito ao conteúdo da proibição de dupla persecução e seus impactos no processo penal brasileiro. Basicamente, o problema a que se pretende responder é: o direito de não ser processado duplamente por fatos já julgados se aplica também em âmbito internacional?
> Em um cenário de globalização e crescente confluência entre ordenamentos jurídicos e até mesmo integrações comunitárias, a temática aqui em debate mostra-se extremamente relevante.
> (...)
> Não restam dúvidas, à vista disso, de que os fatos ora apreciados são coincidentes com os já analisados pelo Estado suíço.
> (...)
> Portanto, se houver a devida comprovação de que o julgamento em outro país sobre os mesmos fatos não se realizou de modo justo e legítimo, desrespeitando obrigações processuais positivas, a vedação de dupla persecução pode ser eventualmente ponderada para complementação em persecução interna.
> Contudo, neste caso concreto não há qualquer elemento que indique dúvida sobre a legitimidade da persecução penal e da punição imposta em processo penal na Suíça por idênticos fatos ao agora denunciados no Brasil. Portanto, a proibição de dupla persecução deve ser respeitada de modo integral, nos termos constitucionais e convencionais. (BRASIL, 2020).

Com efeito, notadamente, o instituto sob análise é capaz de produzir efeitos tanto no âmbito interno quanto no âmbito externo, sendo certo que o *ne bis in idem*, conforme jurisprudência consolidada na Suprema Corte, é dotado, fazendo-se um paralelo com o Direito Ambiental neste ponto, de ubiquidade. Até por isso, esse instituto do Direito deve ser tido como presente em toda a parte e torna necessário com que se tenha uma cooperação entre os povos globais para o seu atendimento (MILARÉ, 2004, p.150).

3.1.2 *Do contexto atual do princípio do "ne bis in idem"*

Apesar de o princípio do *ne bis in idem* ter surgido para solucionar problemáticas afetas ao Direito Civil, é certo que houve uma evolução do instituto que, atualmente, é mais atrelado ao Direito Penal (SABOYA, 2014, p. 39).

Ou seja, as primeiras facetas do cânone em comento restaram modificadas e existiu uma maior interação dos seus efeitos no bojo dos mais demasiados âmbitos do Direito, inclusive, na seara penal.

No Direito Penal, especificamente, o princípio aqui tratado possui o escopo de permitir com que reste atendida, com plenitude, as inteligências contidas nos incisos XXXVI e

XXXIX, ambos do artigo 5º, da Constituição da República. Desse modo, pretendeu-se que, em matéria penal, se tivesse um respeito aos aspectos processuais e materiais do *ne bis in idem*, buscando evitar uma incerteza jurídica relacionada a decisões proferidas por um determinado órgão, bem como trazer uma imperiosidade de que os demais Poderes de Estado, aplicando o princípio da legalidade, respeitassem as decisões provenientes do Judiciário (MASCARENHAS, 2009, p. 3).

Destarte, através do princípio aqui tratado, pode-se afirmar que o intuito da doutrina e jurisprudência pátrias foi fazer ventilar em território brasileiro as garantias dispostas pelas convenções e pactos internacionais que envolviam a matéria de direitos humanos, mormente aquelas disposições observadas no Pacto de São José da Costa Rica, o qual restou firmado pelo Brasil (BRASIL, 1969).

Em outros termos, apesar de inexistir uma expressa previsão no texto constitucional brasileiro, a dupla penalização com base nos mesmos fatos tidos como ilícitos não pode ocorrer em solo nacional. Sobre o tema:

> Tal princípio não está consolidado expressamente em preceito constitucional (se comparado com o modelo constitucional alemão, que o prevê expressamente 3). Porém, o próprio Supremo Tribunal Federal, em decisão do Pleno, cujo acórdão é da lavra do Ministro Ilmar Galvão, ressaltou que: "A incorporação do princípio do ne bis in idem ao ordenamento jurídico pátrio, ainda que sem o caráter de preceito constitucional, vem, na realidade, complementar o rol dos direitos e garantias individuais já previsto pela Constituição Federal, cuja interpretação sistemática leva à conclusão de que a Lei Maior impõe a prevalência do direito à liberdade em detrimento do dever de acusar." (SILVA, 2008, p.2).

Por força dessa ideia, aliás, é que existem no âmbito do Direito Penal diversas teses abordando uma impossibilidade de punição dupla com relação a um mesmo crime. Por exemplo, intenta-se impedir com que diversos tipos penais incidam sobre uma mesma conduta por meio da aplicação da teoria da absorção. Por essa razão é que, na hipótese de ocorrência de um homicídio, não há como se incluir o infrator como praticante de exposição a perigo de vida. Sobre o tema:

> O mesmo se dá na aplicação dos critérios da subsidiariedade e da absorção. No caso do primeiro, se houve processo pelo crime mais grave (tentativa de homicídio, por exemplo), absolvido ou condenado o réu por isso, não poderá ser novamente acusado da prática de exposição a perigo de vida (delito subsidiário, previsto no art. 132, CP), quando se tratar do mesmo fato. No caso de absorção, se o acusado é processado por homicídio e absolvido, não poderá ser novamente acusado da prática de porte ilegal de arma, referentemente ao idêntico fato, já que este crime foi absorvido pelo primeiro. (NUCCI, 2020, p. 628)

O que se tem, portanto, é que, com relação aos mesmos fatos, não há como se buscar a incidência de duas penas na *ultima ratio*.

Ainda, é possível se notar que a absolvição com relação à conduta mais gravosa engloba a acusação relacionada à conduta menos gravosa, de modo que se impede que haja uma espécie de "divisão" da conduta e com que o Estado mantenha uma reserva para perseguir um sujeito em um momento futuro.

Claramente, assim, tem-se um reflexo das premissas provenientes no *ne bis in idem* neste posicionamento doutrinário, pois impede-se uma dupla persecução penal e penalização relacionada a uma mesma conduta.

Em sentido similar, cumpre salientar que o Supremo Tribunal Federal estabeleceu, através da Súmula 241, uma impossibilidade de se aplicar a reincidência penal, simultaneamente, como circunstância agravante e circunstância judicial.

Por fim, é imperioso colocar que existem doutrinadores que defendem que as condições inóspitas de cárcere observadas, conjuntamente com eventuais torturas suportadas por presidiários, devem ser consideradas como uma dupla penalização e, dessa forma, permitirem uma redução da pena (ZAFFARONI; BATISTA; ALAGIA; SLOKAR, 2003, p. 61).

E essa premissa de redução da pena, recentemente, restou acolhida no âmbito do Superior Tribunal de Justiça, o qual, indicando que por meio do Decreto n. 4.463/02, o Brasil reconheceu a competência da Corte Interamericana de Direitos Humanos no que tange à interpretação das normas advindas do Pacto de São José da Costa Rica, decidiu que:

> Como restou asseverado na decisão impugnada, a hipótese dos autos diz respeito ao notório caso do Instituto Penal Plácido de Sá Carvalho no Rio de Janeiro (IPPSC). A referida unidade prisional foi objeto de inúmeras Inspeções que culminaram com a Resolução da Corte IDH de 22/11/2018, que ao reconhecer referido instituto inadequado para a execução de penas, especialmente em razão de os presos se acharem em situação degradante e desumana, determinou no item n. 4, que se computasse "em dobro cada dia de privação de liberdade cumprido no IPPSC, para todas as pessoas ali alojadas, que não sejam acusadas de crimes contra a vida ou a integridade física, ou de crimes sexuais, ou não tenham sido por eles condenadas, nos termos dos Considerandos 115 a 130 da presente resolução".
> (...)
> Nesse ponto, vale asseverar que, por princípio interpretativo das convenções sobre direitos humanos, o Estado-parte da CIDH pode ampliar a proteção dos direitos humanos, por meio do princípio pro personae, interpretando a sentença da Corte IDH da maneira mais favorável possível aquele que vê seus direitos violados.
> (...)
> Ante o exposto, nego provimento ao agravo regimental interposto, mantendo, por consequência, a decisão que, dando provimento ao recurso ordinário em habeas corpus, determinou cômputo em dobro de todo o período em que o paciente cumpriu pena no Instituto Penal Plácido de Sá Carvalho, de 09 de julho de 2017 a 24 de maio de 2019. (BRASIL, 2021)

Com efeito, é certo que as circunstâncias originariamente observadas no princípio do *ne bis in idem* evoluíram e, atualmente, a própria ideia é vista com mais frequência no âmbito do Direito Penal, no qual se pode afirmar que se ultrapassou a perspectiva de que o instituto sob cotejo seria interligado à ideia de coisa julgada e trouxe-se uma perspectiva mais ampla que engloba, até mesmo, uma redução de pena.

3.1.3 *Do princípio do "ne bis in idem" e da sua irradiação no Direito Administrativo*

Além da evolução do instituto para a esfera penal, não há como se olvidar que a ideia do *ne bis in idem* também ressoa no âmbito do Direito Administrativo. É que o ramo do Direito em tela, assim como o Direito Penal, possui uma vertente voltada para a punição e que tem se expandido para diversos setores nos últimos tempos. Aliás:

> Ao punir em âmbito administrativo, o Estado e a sociedade esperam alcançar os mesmos resultados associados à aplicação das penas? A lógica operativa desses institutos – sanções penais e administrativas – pode ser equiparada? A resposta não é simples. Especialmente, porque, como se viu, além das zonas de interseção entre os dois ramos do direito, o exercício do poder punitivo pela Administração Pública se diversificou com enorme rapidez nas últimas décadas. Foram realmente vários os campos por ele apropriados, como os setores de saúde suplementar, dos transportes, financeiro, entre tantos outros. (VORONOFF, 2018, p. 99)

Não obstante ter-se a certeza de que a questão é complexa, a maioria da doutrina compreende que tanto as pretensões punitivas estatais penais e administrativas detém pontos em comum, o que faz com que, por exemplo, sejam aplicadas figuras inerentes ao Direito Penal ao ramo do Direito Administrativo.

É que, dentro das gamas observadas no ramo do Direito Administrativo, verifica-se a existência do denominado Direito Administrativo Sancionador, segundo o qual "a expressão do efetivo poder de punir estatal, que se direciona a movimentar a prerrogativa punitiva do Estado, efetivada por meio da Administração Pública e em face do particular ou administrado" (GONÇALVES; GRILO, 2021, p. 468).

Como consequência disso, cumpre destacar a necessidade de que reste demonstrada uma culpa para que se tente uma busca punitiva na seara administrativa, mormente porque "a repressão administrativa, como a repressão penal, obedece ao princípio da culpabilidade e que as sanções administrativas, como as sanções penais, não podem ser infligidas sem que o comportamento pessoal do autor da infração não tenha revelado uma culpa, intencional ou de negligência" (JUSTEN FILHO, 2015, p. 596)

Por força dessa perspectiva punitiva, a qual se soma com os primados gerais do Direito

de legalidade e tipicidade, é que se tornou natural a compreensão de que não se poderia penalizar duplamente um determinado administrado em razão de um mesmo fato, também, no âmbito da Administração Pública.

Logicamente, em que pese existirem diversos órgãos administrativos, não se pode permitir, em razão da ideia de *ne bis in idem*, que indivíduos sejam penalizados, simultaneamente, em duas vias internas do Poder Público por um mesmo fato (mesmo que se tratem de órgãos diversos).

Apesar de se defender tal premissa, quando do julgamento do Recurso Especial n. 1.138.591/RJ, essa matéria foi observada pelo Superior Tribunal de Justiça. Naquela oportunidade, foi proferido interessante *decisum* em que se observou se seria do Procon, ou da Anatel, a competência para instaurar procedimento administrativo e penalizar prestador de serviços de telefonia atuando às margens da lei.

Diz-se isso, porquanto o recorrente daqueles autos alegou que a multa que lhe foi direcionada pelo órgão de proteção consumerista seria, considerando que é a Anatel a responsável pela vigilância e regulação da atividade comercial de telefonia, inexigível. Ou seja, defendeu-se a existência de incompetência de um órgão quando em cotejo com o outro. Ao analisar a problemática, o Superior Tribunal de Justiça esclareceu que:

> Dessarte, sempre que condutas praticadas no mercado de consumo atingirem diretamente o interesse de consumidores, é legítima a atuação do Procon para aplicar as sanções administrativas previstas em lei, no regular exercício do poder de polícia que lhe foi conferido no âmbito do Sistema Nacional de Defesa do Consumidor. Tal atuação, no entanto, não exclui nem se confunde com o exercício da atividade regulatória setorial realizada pelas agências criadas por lei, cuja preocupação não se restringe à tutela particular do consumidor, mas abrange a execução do serviço público em seus vários aspectos, a exemplo, da continuidade e universalização do serviço, da preservação do equilíbrio econômico financeiro do contrato de concessão e da modicidade tarifária. (BRASIL, 2012)

Veja-se que a Corte Superior, no caso em comento, ressaltou que tanto o Procon quanto a Anatel poderiam atuar na hipótese. Todavia, delimitou-se que o órgão de proteção consumerista deveria se ater a observar os interesses do consumidor e a agência reguladora, por outro lado, somente atuaria em um aspecto macro.

O que se coloca é que, de um raso cotejo, poder-se-ia interpretar o trecho acima transcrito no sentido de que se poderia punir um mesmo fato em dois prismas diversos encontrados na seara administrativa.

Essa ideia poderá trazer uma problemática com relação à Lei Geral de Proteção de Dados Pessoais, porquanto, por meio de uma interpretação sistemática da lei de proteção de

dados e do Decreto n. 2.181/97, não haveria como se permitir, por exemplo, que Procons e Autoridade Nacional de Proteção de Dados punissem um mesmo infrator em âmbitos diversos.

3.2 Do conceito de "conflito de atribuições"

Já buscando destrinchar a problemática evidenciada ao longo do presente trabalho, cabe adentrar nas ideias de conflito de atribuição e, mais adiante, nas nuances relacionadas aos dados pessoais afetas a esta divisão de atribuições, mais especificamente no que diz respeito à multiplicidade de órgãos tratando da matéria e dos efeitos decorrentes de tal situação.

Pois bem. As primeiras considerações relacionadas ao conflito de atribuições podem ser visualizadas no âmbito brasileiro quando da promulgação da Constituição de 1891, a qual teve como inspiração o constitucionalismo norte-americano em sua concepção de federalismo (FEIJÓ, 2012, p. 2-3).

Ao estudar as origens do tema que veio a ser importado para o Brasil, Rui Barbosa esclareceu que o povo norte americano sempre possuiu uma desconfiança com relação a uma centralização de poder, porquanto, desde os idos de resistência à Inglaterra, já esboçavam essas posições. Confira-se:

> Ora, os americanos, nosso padrão nesse trabalho, que hoje rege o país (ao menos nominalmente), sempre destinguiram um profundo apêgo à liberdade individual e uma desconfiança invencível contra todo o poder, fôsse qual fôsse. Aos seus olhos, as assembléias eletivas não ofereciam mais segurança do que um rei hereditário, e o arbítrio de umas não é menos formidável do que o absolutismo do outro. Estava-lhes em mente a lembrança da resistência, que tinham tido que opor ao parlamento inglês, em defesa dos seus direitos e interêsses. Diante dêles se erguia a memória do monstruoso egoísmo e da néscia obstinação, com que os lords e comuns se avieram por tanto tempo em sua política colonial. E sentimentos tão vivazes não podiam deixar de exercer acentuada influência na Constituição dos Estados Unidos. (BARBOSA, 1953, nota 37).

Nesse contexto, é que, buscando sanar os receios da sociedade americana e que foi ressado no ordenamento brasileiro, é que se previu a separação do exercício do poder (ESTADOS UNIDOS DA AMÉRICA, 1803), de modo que passaram a ser considerados inconstitucionais os atos proveniente de autoridades que não tinham competência para os editar.

A partir dessa premissa, obviamente, deverá se evitar trazer dúvidas acerca de quem será a autoridade responsável por analisar uma problemática no âmbito do Direito Administrativo.

Adentrando-se em uma análise mais profícua a respeito da temática, José Cretella

Júnior (1985, p. 17) menciona que o que se precisa impedir é o confronto entre duas autoridades administrativas que se entendem competentes para analisar uma determinada matéria.

E essa situação pode ter um cunho positivo, quando se encontra diante de hipótese em que duas autoridades simultaneamente se julgam competentes para analisar uma problemática, quanto negativa, a qual pode ser observada quando existe um vácuo no que tange à competência de análise de uma determinada matéria administrativa.

Do mesmo modo, é possível falar-se em conflitos de atribuições internos, consistente nas hipóteses em que se tem duas autoridades que entendem pela sua competência ou incompetência no âmbito de um mesmo Poder, e em conflitos externos, podendo ser ilustrados como sendo circunstâncias em que a competência ou incompetência é debatida por autoridades que se situam em Poderes diversos (CRETELLA JÚNIOR, 1985, p. 18)

Perceba-se que esse tipo de choque de atribuição destoa do que se denomina "conflito de competência", porquanto, enquanto no primeiro pode existir uma dúvida relacionada à autoridade responsável por uma análise de matéria em cotejo com um membro do Poder Judiciário ou outra autoridade administrativa, no segundo cotejo somente se pode falar em uma discussão com relação a duas autoridades judiciárias (CRETELLA JÚNIOR, 1985, p. 20).

De todo modo, não há como se olvidar que todas as questões que envolvem a responsabilidade de dirimir um requerimento devem ser solucionadas com a maior brevidade. Afinal, tendo em vista a previsão de direito de petição e de resposta contida na alínea "a", do inciso XXXIV, do artigo 5º, da Constituição da República, não se pode permitir com que um administrado não tenha seus pleitos e defesas sopesados no âmbito administrativo.

Portanto, seja proveniente do proferimento de decisão questionável ou de uma ausência de decisão, é extremamente prejudicial a questão relacionada ao conflito de atribuições aqui em lume.

3.3 Conflito de atribuições junto aos órgãos consumeristas

Sabendo-se que as técnicas de comércio na via online se utilizam de dados pessoais para fornecer produtos a consumidores que estejam navegando por sítios eletrônicos, é notório que questões envolvendo esses bens jurídicos terão um debate tanto de índole consumerista quanto no campo da proteção de dados.

Tendo essa perspectiva em mente, é importante se evitar que duas autoridades, no caso

uma com espeque de órgão de defesa do consumidor e a Autoridade Nacional de Proteção de Dados, punam duplamente uma infração interligada a esta forma de *marketing* em meio virtual.

Por essa razão, faz-se *mister* com que sejam abordadas as intersecções entre as atuações provenientes de entidades que possuem como escopo uma defesa de direitos de lavra consumerista e a autoridade protetiva de dados, o que somente é possível ao se destrinchar esses dois tipos de órgãos.

3.3.1 *As atividades dos órgãos de proteção ao consumidor*

Conforme se observou, existiu uma evolução dos direitos adquiridos por administrados em escala mundial. Em uma primeira vertente, se teve a obtenção de direitos civis e, posteriormente, direitos políticos. Em seguida, os cidadãos obtiveram os direitos sociais, porquanto teve-se uma perspectiva de responsabilidade social muito presente nos ordenamentos jurídicos (SROUR, 2000, p. 196).

Dentre os direitos sociais, pode-se encontrar a proteção de ordem consumerista. Isso porque, ao buscar atender a expressa dicção do inciso XXXII, da Constituição Federal, é que o legislador pátrio promulgou o Código de Defesa do Consumidor.

Além disso, até mesmo diante da importância de se limitar as atividades econômicas, é que se entende que o Direito Consumerista atingiu o status de um microssistema, ou seja, sobrevindo uma normativa que elucide novos direitos para proteger a parte de uma relação jurídica, existe uma espécie de somatório daquela inteligência legal ao que já constava no Código de Defesa do Consumidor.

Desse modo, sabendo-se desse caráter de adição, aplicar-se-iam diversas leis em prol das pessoas enquadradas no conceito de consumidor (BRASIL, 2010).

No intuito de permitir com que esses direitos fossem atingidos, por óbvio, o Poder Público instituiu órgãos e entidades que tinham como função assegurar que houvesse respeito aos consumidores.

É daí que surgiram, por exemplo, os Procons, a Secretaria Nacional do Consumidor, o Departamento de Proteção e Defesa do Consumidor e as demais entidades (ainda que em uma vertente específica dentro de um determinado Poder ou órgão) que fazem parte do Sistema Nacional de Defesa do Consumidor. Todas essas figuras foram advindas da necessidade de se atender às premissas visualizadas no artigo 44, do Código de Defesa do Consumidor, a propósito:

> Criou o Sistema Nacional de Defesa do Consumidor – SNDC, congregando os órgãos federais, estaduais, do Distrito Federal e municipais, que direita ou indiretamente exercem atividades relacionadas com a defesa do consumidor, indicando, portanto, que esses órgãos devem estar reunidos num sistema, permitindo sua integração e cooperação mútua. (GRINOVER, 2011, p. 816)

Assim, existem órgãos que atuam em âmbitos municipais, estaduais e federal com vistas a tutelar os direitos de adquirentes de serviços e produtos. Essa situação, por si só, faz com que se tenha dúvidas acerca da autoridade responsável pela análise de uma determinada reclamação.

Diz-se isso, porquanto já há uma discussão relacionada a quem deve recair a análise de um determinado questionamento, se ao Procon Municipal ou ao Procon Estadual.

Esse ponto é controverso, pois, a rigor, inexiste hierarquia entre os diversos órgãos que compõem o Sistema Nacional de Defesa do Consumidor (ZULIANI, 2011, p. 987) e o artigo 5º, do Decreto 2.181/97, dispõe que "qualquer entidade ou órgão da Administração Pública, federal, estadual e municipal, destinado à defesa dos interesses e direitos do consumidor, tem, no âmbito de suas respectivas competências, atribuição para apurar e punir infrações a este Decreto e à legislação das relações de consumo".

Com efeito, a toda evidência poder-se-ia ter uma situação em que, exemplificadamente, existam dois procedimentos administrativos acerca de um mesmo fato, um em trâmite em um Procon Municipal e outro em um Procon Estadual.

Todavia, considerando o já abordado princípio do *ne bis in idem*, há que se entender pela necessidade de reunião de eventuais procedimentos administrativos que possuam os mesmos contornos, de modo a aplicar-se as inteligências visualizadas no quanto disposto pelos artigos 15 e 16, do Decreto 2.181/97.

De todo modo, fato é que não há uma adequada coordenação entre os órgãos de consumo, o que tem feito com que fornecedores sejam penalizados por uma mesma conduta em dois procedimentos administrativos que possuem andamentos em diferentes esferas. Isso, aliás, é visto desde o longínquo ano de 2010, no qual o Superior Tribunal de Justiça, ao analisar o Recurso Especial n. 1.087.892/SP, pontuou que:

> Na espécie, foram instaurados dois processos administrativos, um pelo Departamento de Proteção e Defesa do Consumidor amparado no artigo 10, § 1º, do CDC, e outro pela Fundação de Proteção e Defesa do Consumidor do Estado de São Paulo fundamentado nos artigos 8º e 10, caput, do CDC, ensejando a aplicação de multas pelos referidos órgãos.
> Conforme ficou consignado do acórdão recorrido: "Confronto das situações previstas pelos § 1º, do artigo 10, e 8º e 10 "caput", do Código do Consumidor, que se excluem, não coexistem e, como tal, não podem ser, cumulativamente, sancionadas." Logo, a recorrida foi punida pelos dois órgãos de defesa do consumidor em face da mesma infração à legislação consumerista. Não obstante os

> órgãos de proteção e defesa do consumidor, que integram o Sistema Nacional de Defesa do Consumidor, serem autônomos e independentes quanto à fiscalização e controle do mercado de consumo, não se demonstra lícito e nem razoável a aplicação de sanções, pela mesma infração, por mais de uma autoridade consumerista, uma vez que tal conduta possibilitaria que todos os órgãos de defesa do consumidor existentes no País punissem o infrator, desvirtuando o poder punitivo do Estado (BRASIL, 2010).

Se em um mesmo microssistema já se tem uma celeuma de atribuição e dupla penalização, é plausível que, ao serem incluídas novas questões relacionadas à proteção de dados em matéria consumerista, sejam visualizadas ainda mais problemáticas com esse caráter.

3.3.2 *Pontos de convergência entre as atribuições dos órgãos de proteção ao consumidor e da Autoridade Nacional de Proteção de Dados*

Conforme já restou esboçado, existem situações que envolvem proteção de dados pessoais que se comunicam com as premissas consumeristas. Isso porque, até mesmo considerando o previsto no artigo 2º, VI, da Lei Geral de Proteção de Dados Pessoais, um dos fundamentos da normativa protetiva de dados é a defesa do consumidor.

Ora, em diversos casos, ao adquirir algum produto, um comprador precisa realizar um cadastro em sítes de *e-commerce* e, logicamente, isso envolve o fornecimento de dados pessoais, tais como o cadastro nacional de pessoas físicas, o número de telefone, ano de nascimento.

Esse fornecimento de dados, por si só, permite com que o fornecedor de produtos e serviços se utilize das práticas denominadas *data-driven marketing* e *profiling*, nas quais, por meio de dados e compras pretéritas, o vendedor consegue antever o padrão de vida do consumidor e lhe apresentar, na via digital, anúncios com produtos que lhe podem ser interessantes (ZANATTA, 2019, p. 4 – 5).

A maior exemplificação dessas práticas é a notícia de que a Target, loja de departamentos norte-americana, fez uma campanha onde as suas clientes a informavam o estado de gravidez e indicavam a data estimada de nascimento das crianças.

Com tais informações em seu poder, a referida loja passou a observar os hábitos das mulheres grávidas e concluiu que a compra de cremes, perfumes e suplementos crescia durante o período da gestação. Esses hábitos de compra permitiram, assim, que a Target percebesse, mesmo sem uma informação explícita fornecida por uma determinada cliente, a condição de gestante de suas compradoras e, assim, pudesse fornecer produtos atrelados a este período de

vida, tais quais carrinhos para bebês, fraldas e outros (DUHIGG; POLE, 2012).

Nas mesmas conjunturas, empresas podem se utilizar do que se denominou chamar de *geoblocking* e *geopricing*. Tais práticas, em um breve escorço, consistem, respectivamente, em, de acordo com a localização de determinados consumidores, bloquear uma oferta disponibilizada em meio eletrônico e alterar os preços cobrados por um mesmo produto (FÁVARO, 2018).

Inclusive, por conta destes tipos de conduta, é que a Decolar.com foi punida pelo Departamento de Proteção e Defesa do Consumidor e, conseguintemente, teve que realizar o pagamento de uma multa na ordem de sete milhões e meio de reais (BRASIL, 2018).

Apenas dos exemplos acima trazidos se percebe que os tipos de operação em comento são controversos, pois trazem implicações de diversas naturezas informacionais, anti-discriminatórias e dialógica. Confira-se:

> O argumento principal do artigo é que a perfilização é um ato sócio-técnico que desencadeia uma série de obrigações jurídicas, com contornos jurídicos identificáveis na nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018). A ação de "encaixar uma pessoa", a partir de seus dados pessoais, em um perfil social e inferir algo sobre ela implica em obrigações de três naturezas: (i) informacional, relacionada à obrigação de dar ciência da existência do perfil e garantir sua máxima transparência, (ii) anti-discriminatória, relacionada à obrigação de não utilizar parâmetros de raça, gênero e orientação religiosa como determinantes na construção do perfil, e (iii) dialógica, relacionada à obrigação de se engajar em um "processo dialógico" com as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e de como decisões são tomadas (ZANATTA, 2019, p. 3).

Conquanto algumas das referidas implicações já fossem abarcadas no Código de Defesa do Consumidor e na Lei do Cadastro Positivo, é certo que a norma que transplantou, de uma forma direta e com base no regramento europeu, a proteção de dados em território nacional trouxe uma nova perspectiva.

É dizer, enquanto já se tinha um abarcamento dos pontos informacionais e anti-discriminatória, sobreveio a exigência de que fossem trazidas fundamentações capazes de explicitar aos detentores de dados os motivos que levaram à sua perfilização (GOODMAN; FLAXMAN, 2017, p. 5 – 6).

Apesar de não se ter uma problemática no tratamento de dados atrelados ao *data-driven marketing* e ao *profiling* na hipótese de concordância do detentor dos referidos bens, por certo poderão existir celeumas com relação a artigos presentes tanto no Código Consumerista quanto na própria Lei Geral de Proteção de Dados Pessoais. Afinal, é possível que se tenha um excesso de propagandas por parte do fornecedor de produtos, bem como que um determinado usuário de serviços *online* não tenha as devidas informações com relação à

destinação de seus dados pessoais.

Ou seja, é factível que sejam observadas condutas que consistam em infrações tanto aos ditames dos artigos 36, juntamente com seus parágrafos, 39 e 43, §1º, do Código de Defesa do Consumidor quanto ao que resta previsto no artigo 6º, I e VI, da Lei Geral de Proteção de Dados Pessoais, bem como à vedação ao uso discriminatório de dados contidos naquela normativa. Desse modo, percebe-se que tanto os órgãos que possuem como tutela a proteção dos direitos dos denominados consumidores quanto o órgão que tem como objeto a defesa dos dados pessoais poderiam atuar nesse caso.

Nas mesmas conjunturas, uma pessoa atingida por uma irregularidade tem a premissa de formular um questionamento que envolva o mal uso de seus dados no âmbito de duas autoridades administrativas.

Antevendo essa situação problemática, é que a Autoridade Nacional de Proteção de Dados e a Senacon, órgão que integra o Ministério da Justiça e possui o objetivo de coordenar as políticas de defesa do consumidor, firmaram acordo de cooperação técnica que estabeleceu uma união para que fossem promovidas ações de:

> a) Apoio institucional e intercâmbio de informações relativas às suas respectivas esferas de atuação;
> b) Compartilhamento de informações agregadas e de dados estatísticos quanto a reclamações de consumidores relacionadas à proteção de dados pessoais, em especial aquelas registradas no Sistema Nacional de Informações de Defesa do Consumidor - SINDEC e nas bases de dados do Consumidor.gov.br;
> c) Uniformização de entendimentos e coordenação de ações, inclusive no que tange ao endereçamento de reclamações de consumidores e à atuação no caso de incidentes de segurança envolvendo dados pessoais de consumidores;
> d) Desenvolvimento de indicadores conjuntos relacionados à proteção de dados pessoais no âmbito de relações de consumo;
> e) Elaboração conjunta e intercâmbio de estudos, análises, notas técnicas e projetos de pesquisa sobre direitos do consumidor e proteção de dados pessoais;
> f) Desenvolvimento, organização e promoção de ações conjuntas de formação e de capacitação, incluindo cursos, seminários e elaboração de materiais informativos; e
> g) Cooperação quanto a ações de fiscalização relacionadas à proteção de dados pessoais no âmbito das relações de consumo (BRASIL, 2021).

Nessa direção, ainda que restem pendentes as tomadas de medidas para implementação do pacto em pauta, é possível se inferir que, ao se estabelecer um “endereçamento de reclamações”, existiu uma busca de evitar-se uma penalização dupla de um infrator.

Além desses contornos, cabe rememorar que o Ministério Público, também, detém a competência para propor ações e procedimentos que tenham como escopo a defesa dos direitos consumeristas, desde que, claro, sejam tutelados interesses difusos, coletivos ou individuais homogênios.

Ou seja, além da possibilidade de punição pelo Procon e Autoridade Nacional de Proteção de Dados, é possível que um agente que atue em desacordo com a Lei Geral de Proteção de Dados Pessoais enfrente um inquérito civil e, posteriormente, ação judicial, que vise a apuração de tal conduta. Essa linha de raciocínio, inclusive, já foi abordada por Rafael Zanatta, o qual consignou que:

> É evidente, portanto, que tanto o MP quanto as associações civis poderão ajuizar ações civis públicas para proteção de dados pessoais para proteção de direitos difusos, como já tem ocorrido em diversos exemplos, como no caso da pioneira ação do Instituto Brasileiro de Defesa do Consumidor contra a ViaQuatro (caso das Portas Interativas Digitais, que não será aprofundado aqui) (RINALDI, 2018) ou na ação do MPDFT contra o Banco Inter (incidente de segurança) (PAYÃO, 2018). A partir da leitura conjunta do art. 22 com o art. 42 da LGPD de forma íntegra ao sistema jurídico brasileiro, pode-se afirmar com segurança que a legislação brasileira (i) permitirá uma atuação repressiva, em nível administrativo, para a tutela da proteção de dados pessoais, valendose do microssistema de proteção dos direitos difusos, (ii) fomentará a atuação de entidades civis especializadas e do MP na tutela dos direitos difusos de proteção de dados pessoais, por meio do Poder Judiciário, e (iii) possibilitará o uso de um ferramental do processo civil brasileiro para interrupção de violações de direitos assegurados na LGPD, tornando a dinâmica regulatória mais complexa (ZANATTA, 2019, p. 359).

Dessa forma, apesar de existirem tentativas para evitar-se o risco de que se tenha uma dupla penalização de agentes por descumprimento da lei protetiva de dados, é certo que a celeuma carece de maiores estudos, bem como de normativas mais efetivas que impeçam a ocorrência de *bis in idem*.

3.4 Conflito de atribuições junto ao CADE

Ainda dentro do bojo da Lei de Proteção de Dados Pessoais, é certo que os bens jurídicos ali tutelados podem ser utilizados com a finalidade de trazerem uma vantagem concorrencial a uma determinada empresa, quando em cotejo com os seus concorrentes. Nesse contexto, é palpável que o uso indevido de dados pessoais poderá trazer problemas capazes de serem sopesados tanto pelo Conselho Administrativo de Defesa Econômica (CADE) quanto pela Autoridade Nacional de Proteção de Dados.

3.4.1 *As atividades do CADE*

O Conselho Administrativo de Defesa Econômica surgiu no ano de 1962, quando o Presidente João Goulart, por meio da sanção da Lei n. 4137/1962, previu que esta figura seria instituída e teria uma subordinação ao Ministério da Justiça.

Estabeleceu-se, naquele momento, que a instituição em lume teria como funções principais a gestão econômica e contábil das empresas governamentais.

Ou seja, a primeira atuação do conselho em evidência, até mesmo em razão dos contornos do regime militar observado à época, foi tímida (DOS SANTOS; JÚNIOR; ZANIN, 2017, p. 192).

Em 1994, com a sobrevinda da Lei n. 8884/94, se trouxe uma maior possibilidade de que o Conselho Administrativo de Defesa Econômica atuasse de forma mais efetiva, em especial porque se estabeleceu que aquela figura seria uma autarquia.

Apenas pelo fato de ser uma autarquia, já se nota uma maior independência do CADE. Diz-se isso, pois, como é sabido, as autarquias possuem uma capacidade de se autoadministrar com relação às matérias específicas que o ente que as criou indicou (DI PIETRO, 2020, p. 974).

Apesar dessas primeiras menções ao CADE, é cediço que, no início dos anos 90, observou-se uma privatização de diversas instituições estatais, o que fez com que o Brasil abandonasse uma função que outrora exercia de uma espécie de Estado empresário, ou seja, que atuava diretamente no mercado concorrencial no fornecimento de produtos e serviços ao consumidor (FARINA, 1996, p. 37).

Em outros termos, o Brasil passou a deixar de atuar na condição de fornecedor e, visando a preservarção do ambiente competitivo e combater aquelas condutas que são contrárias a tal premissa, restou instaurada uma política mais efetiva de controle mercadológica.

É por isso que, em 2011, sobreveio a Lei n. 12.529/2011, a qual alterou a estrutura do Conselho Administrativo de Defesa Econômica e trouxe uma nova gama de atividades a serem exercidas por aquela pessoa jurídica de direito público. Afinal, naquele ato normativo, percebe-se que foram ventiladas previsões mais específicas à indigitada entidade, mormente para fins de que fosse responsável pela criação de resoluções, julgar e tratar de processos cujo pano de fundo fosse decorrente de uma discussão concorrencial.

Portanto, as atribuições do Conselho Administrativo de Defesa Econômica, de certo modo, foram majoradas para que, notadamente, houvesse a possibilidade de se ter um efetivo controle da livre iniciativa trazida pelo artigo 170, da Constituição da República mais recente.

Nessas conjunturas, por exemplo, cabe ao Conselho Administrativo de Defesa Econômica exercer funções em três vias essenciais, quais sejam, informativa, repressiva e preventiva junto ao mercado.

A primeira, que pode ser conhecida como sendo educacional e pode ser encontrada nos

artigos 9º, XIV e 13, XV da Lei 11.529/11, é exercida, de forma exemplificada, quando CADE traz instruções ao público que se relacionem às práticas que prejudicam o andamento sadio do mercado (DOS SANTOS; JÚNIOR; ZANIN, 2017, p. 193).

Por sua vez, a perspectiva preventiva exercida pela autarquia diz respeito à realização de uma análise e decisão de atos de concentação que podem trazer um prejuízo à livre concorrência. Assim, o que faz o CADE é sopesar se uma determinada fusão pode prejudicar o mercado, de modo que as operações econômicas sejam aquelas envolvendo pessoas físicas ou jurídicas de direito público e privado, encontram-se sob o atento olhar daquela instituição (DOS SANTOS; JÚNIOR; ZANIN, 2017, p. 193.

Finalmente, a função repressiva consiste na aplicação de sanções quando um determinado agente infringir o quanto disposto pelo artigo 36, da Lei n. 12.529/2011, o qual prevê que:

> Art. 36. Constituem infração da ordem econômica, independentemente de culpa, os atos sob qualquer forma manifestados, que tenham por objeto ou possam produzir os seguintes efeitos, ainda que não sejam alcançados:
> I - limitar, falsear ou de qualquer forma prejudicar a livre concorrência ou a livre iniciativa;
> II - dominar mercado relevante de bens ou serviços;
> III - aumentar arbitrariamente os lucros; e
> IV - exercer de forma abusiva posição dominante. (BRASIL, 2011).

Da leitura do artigo acima transcrito, é possível se concluir que, ao controlar os dados pessoais de diversos clientes, uma determinada empresa poderia incorrer em práticas que dificultem uma livre concorrência.

E essa afirmativa é simples, especialmente ao se ter em mente que a ciência com relação aos hábitos de consumo de determinadas pessoas pode permitir com que um comerciante saia na frente de seu concorrente.

É dizer que um uso irregular dos dados pessoais pode fazer com que um infrator seja investigado dentro do Conselho Administrativo de Desenvolvimento Econômico e, também, da Autoridade Nacional de Proteção de Dados.

3.4.2 *Pontos de convergência entre as atribuições do CADE e da Autoridade Nacional de Proteção de Dados*

Não há como se olvidar que os dados pessoais, atualmente, são elementos econômicos extremamente importantes; eis que os mercados *online* estão tendo uma preferência do público

em geral.

Estudos demonstram que os mercados considerados “digitais” possuem as mesmas características do comércio tradicional, contudo, possuem acréscimos que os tornam uma estrutura única, quais sejam, uma rede envolvendo economia de escala, menores custos marginais e prestação de serviços de forma mais ampla e simplificada (CENTER, 2019, p. 6).

Outrossim, é plausível se concluir que a observância da *big data* permite com que determinadas empresas direcionem de forma mais eficaz produtos aos usuários. Essa temática, inclusive, restou sopesada no âmbito da Federal Trade Commission, a grosso modo uma espécie de CADE norte-americano, quando da aquisição da empresa Double Click, plataforma de anúncios digitais, pelo Google em 2007.

Apesar de na oportunidade ter se permitido a referida aquisição, é certo que a Conselheira Pamela Jones Harbour bem apontou que a operação em pauta daria ao Google, o qual já detinha uma série de de usuários angariadas por meio de *cookies*, uma extrema vantagem competitiva na área do *marketing* e sugeriu uma análise mais detida acerca da problemática que foi apresentada (ESTADOS UNIDOS DA AMÉRICA, 2007).

Ou seja, as mesmas práticas que foram abordadas como sendo passíveis de ferirem a legislação consumerista brasileira, também, poderão obstar com que o mercado tenha um regular andamento. É que, por óbvio, uma determinada empresa que detenha as informações necessárias para proceder com o *profiling* possui maiores chances de atingir o destinatário final de seus produtos, pois, como já dito, o *marketing* eletrônico é, de certa forma, mais direcionado.

Essa premissa prejudica a competição, por exemplo, de duas empresas que anunciam nas plataformas eletrônicas, quando uma possui um serviço prestado com base na colheita e tratamento de usuários e outra não.

E mais, é certo que uma determina empresa que adquira outras, o que envolveria o cadastro dos costumeiros consumidores, poderia dominar um determinado mercado.

Por essas razões, é que pode-se afirmar que, em alguns casos, tanto o CADE quanto a Autoridade Nacional de Proteção de Dados Pessoais poderão atuar.

Buscando evitar essa situação problemática de competência, há que se destacar que a Autoridade Nacional de Proteção de Dados firmaram o acordo de cooperação técnica n. 5/2021 em que pontuam, de forma direta, que se trata de um documento que tem o escopo de “viabilizar ações a serem adotadas pelas partes, de forma conjunta e coordenada, quando da ocorrência de situações que interseccionam ambas as esferas de competências” (BRASIL, 2021).

Novamente, portanto, pode-se dizer que a atitude de ambas as instituições é válida, contudo, carecem contornos mais nítidos acerca de quais serão as situações em que existirá uma possibilidade de conflito de atribuições.

Em outros termos, trata-se apenas de um passo inicial que, certamente, precisará evoluir para fins de ser apto a impedir uma punição dúplice, a um determinado infrator da lei, protetiva de dados pessoais.

3.5 Conflito de atribuições junto ao BACEN

Não é possível ventilar-se dúvidas no sentido de que entre os mais diversos dados pessoais encontrados na *big data* estão incluídos aqueles dados que foram direcionados às instituições bancárias, tais quais movimentação financeira, condições econômicas e outras.

Por isso é que há de se abordar a possibilidade de que um eventual vazamento de dados em tal âmbito possa vir a ser objeto de cotejo em dois âmbitos diversos, quais sejam, no bojo do Banco Central e no bojo da Autoridade Nacional de Proteção de Dados.

3.5.1 *As atividades do BACEN*

Os Bancos, sem sombra de dúvidas, convivem em um sistema extremamente competittivo, mormente porque, além do surgimento de *fintechs* atuando no setor, as atividades relacionadas ao financiamento de objetos de consumo e de fornecer recursos às empresas contam com uma grande gama de personagens atuando (ANDREZO; LIMA, 2002, p. 1).

Buscando, assim, estabelecer limites com relação à atividade bancária é que, no ano de 1964, houve a criação do Banco Central. Essa figura se trata de uma autarquia, formada através de recursos próprios e vinculada ao Ministério da Fazenda. A propósito:

> A criação do Banco Central do Brasil (BACEN) ocorreu em 31 de dezembro de 1964 com o Decreto-Lei n. 4.595. A iniciativa do Brasil na criação de seu Banco Central foi tardia, realizada há apenas 46 anos. O primeiro país a adotar a instituição foi a Inglaterra, em 1694. Os principais objetivos dessa criação foram os seguintes109: 1) zelar pela adequada liquidez da economia; 2) manter as reservas internacionais do País, em nível adequado; 3) estimular a formação de poupança em níveis adequados às necessidades de investimento do país; e 4) zelar pela estabilidade e promover o permanente aperfeiçoamento do Sistema Financeiro Nacional (PORTO; GONÇALVES; SAMPAIO, 2012, p. 69)

Ou seja, inicialmente, o Banco Central tratou-se de uma espécie de “evolução” da

outrora vista Superintendência da Moeda e do Crédito que anteriormente restava responsável pela organização das políticas de controle monetário, controle de bancos e fomento econômico (MATTA, 2002, p. 7).

É certo que, com o passar dos anos, a entidade aqui tratada precisou, até mesmo em razão do novo texto constitucional, se adaptar ao que lhe foi atribuído.

Diz-se isso, porquanto, após a Constituição da República de 1988, pode-se falar que existiram melhores apontamentos com relação à atuação do Banco Central. Inclusive, sobre o tema:

> Hoje podemos relacionar suas competências como sendo as seguintes: 1) a emissão de dinheiro seja em papel ou em moeda metálica; 2) efetivação dos serviços de meio circulante; 3) recolhimentos compulsórios dos bancos comerciais; 4) cumprir operações de desconto e empréstimos de assistências à liquidez as instituições financeiras; 5) ajustar a execução dos serviços de compensação dos cheques e dos outros papéis; 6) executar operações de compra e venda de títulos públicos federais (política monetária); 7) autorizar, normatizar, fiscalizar e intervir nas instituições financeiras; e 8) controlar o fluxo de capitais estrangeiros, garantindo o correto funcionamento do mercado cambial (PORTO; GONÇALVES; SAMPAIO, 2012, p. 72).

Além desses pontos, incumbe ao Banco do Brasil estudar as atuações dos bancos, regular o mercado e, por consequência, ser vigilante no que tange à tomada de medidas que são necessárias para que se mantenha a saúde do sistema financeiro, bem como conduzir processos administrativos em que figurem pessoas físicas e jurídicas que atuem em desacordo aos objetivos aqui tratados (MATTA, 2002, p. 12).

Em razão disso, aliás, é que o Banco Central detém a competência para editar circulares e resoluções que visem manter com que o sistema financeiro permaneça saudável, especialmente diante da necessidade, a qual é proveniente de uma evolução rápida, de revisitar matérias reguladas.

Dentre as matérias reguladas, por certo, a autarquia em pauta, há muito, já discorria acerca de questões que, mesmo que de forma indireta, envolviam o tratamento de dados pessoais.

3.5.2 *Pontos de convergência entre as atribuições do BACEN e da Autoridade Nacional de Proteção de Dados*

Como já colocado, o Banco Central, há anos, já possui resoluções e circulares que envolvem situações atreladas aos dados pessoais. E isso, aliás, vem sendo reconhecido pelo

Poder Judiciário em processos que discorrem acerca de vazamento de dados financeiros. Sobre o que se ventila, vide posição do Tribunal de Justiça do Estado de São Paulo onde se lê que:

> Ora, com o devido respeito, a situação descrita na petição inicial é grave por demonstrar a falta de segurança a que foram submetidos dados bancários sensíveis dos autores. A demora na comunicação do golpe ao banco réu apenas reforça isso, já que esta se deve à fé que os autores depositaram nos meliantes em razão da confirmação de seus dados pessoais que, a rigor, deveriam ser de posse tão-somente da Instituição Financeira (SÃO PAULO, 2019, p. 6-7).

Ou seja, quase que todos os atos administrativos provenientes do Banco Central que tratem, exemplificadamente, de movimentação bancária entre pessoas físicas são considerados atos que versem a respeito de dados pessoais.

Com isso em mente, pode-se falar que a Circular BACEN n. 3.978, a qual instituiu uma obrigação aos bancos relacionada à implementação de políticas e procedimentos internos de controle que sejam aptos a impedirem crimes, envolve proteção de dados.

Diz-se isso, pois nos parágrafos do artigo 28 daquele ato consta que as "instituições referidas no art. 1º devem manter registros de todas as operações realizadas, produtos e serviços contratados, inclusive saques, depósitos, aportes, pagamentos, recebimentos e transferências de recursos" e, em seguida, dispõe que tais registros devem, minimamente, conter alguns dados pessoais.

Do mesmo modo, é certo que a Circular BACEN n. 4.001, que elencou práticas que poderiam ser consideradas indícios de crime em âmbito financeiro, também previu pontos que tratam de dados pessoais.

Afinal, naquela normativa podem ser vistas especificações que tratam de situações problemáticas que tenham relação com dados cadastrais dos clientes, que nada mais são que dados pessoais. A propósito:

> Art. 1º As operações ou as situações descritas a seguir exemplificam a ocorrência de indícios de suspeita para fins dos procedimentos de monitoramento e seleção previstos na Circular nº 3.978, de 23 de janeiro de 2020:
> (...)
> III - situações relacionadas com a identificação e qualificação de clientes:
> a) resistência ao fornecimento de informações necessárias para o início de relacionamento ou para a atualização cadastral;
> b) oferecimento de informação falsa;
> c) prestação de informação de difícil ou onerosa verificação;
> d) abertura, movimentação de contas ou realização de operações por detentor de procuração ou de qualquer outro tipo de mandato;
> e) ocorrência de irregularidades relacionadas aos procedimentos de identificação e registro das operações exigidos pela regulamentação vigente;
> f) cadastramento de várias contas em uma mesma data, ou em curto período, com depósitos de valores idênticos ou aproximados, ou com outros elementos em comum, tais como origem dos recursos, titulares, procuradores, sócios, endereço, número de

> telefone, etc.;
> g) operações em que não seja possível identificar o beneficiário final, observados os procedimentos definidos na regulamentação vigente;
> h) representação de diferentes pessoas jurídicas ou organizações pelos mesmos procuradores ou representantes legais, sem justificativa razoável para tal ocorrência;
> i) informação de mesmo endereço residencial ou comercial por pessoas naturais, sem demonstração da existência de relação familiar ou comercial;
> j) incompatibilidade da atividade econômica ou faturamento informados com o padrão apresentado por clientes com o mesmo perfil;
> k) registro de mesmo endereço de e-mail ou de Internet Protocol (IP) por diferentes pessoas jurídicas ou organizações, sem justificativa razoável para tal ocorrência;
> l) registro de mesmo endereço de e-mail ou Internet Protocol (IP) por pessoas naturais, sem justificativa razoável para tal ocorrência;
> m) informações e documentos apresentados pelo cliente conflitantes com as informações públicas disponíveis;
> n) sócios de empresas sem aparente capacidade financeira para o porte da atividade empresarial declarada;
> IV - situações relacionadas com a movimentação de contas de depósito e de contas de pagamento em moeda nacional, que digam respeito a:
> a) movimentação de recursos incompatível com o patrimônio, a atividade econômica ou a ocupação profissional e a capacidade financeira do cliente;
> (...)
> c) movimentação de recursos de alto valor, de forma contumaz, em benefício de terceiros;
> d) manutenção de numerosas contas destinadas ao acolhimento de depósitos em nome de um mesmo cliente, cujos valores, somados, resultem em quantia significativa;
> e) movimentação de quantia significativa por meio de conta até então pouco movimentada ou de conta que acolha depósito inusitado;
> (...)

Além de tais pontos, cabe ressaltar que são tratadas circunstâncias que envolvem transferências de valores a pessoas não identificadas adequadamente, é dizer, sem dados pessoais disponibilizados à instituição bancária em atividade.

Evidentemente, portanto, existirão situações em que um banco, ao ignorar as Cartas-Circulares supracitadas, estará sujeito a penalidades provenientes de processo administrativo que tramita junto ao Banco Central e, também, no âmbito da Autoridade Nacional de Proteção de Dados.

Buscando evitar problemáticas relacionadas aos dados pessoais, e consequentemente uma incursão de uma instituição na esfera de atuação da Autoridade Nacional de Proteção de Dados, é que, por meio da Circular n. 4.015 e da Resolução Conjunta n. 1/2020, se trouxe o denominado *open banking*.

Por meio do *open banking*, ter-se-á uma possibilidade de que bancos e *fintechs* desenvolvam aplicativos que permitam com que os seus clientes tenham uma maior liberdade com relação aos serviços que recebem por meio de *Application Programming Interface* abertas, ou seja, interfaces que possibilitam uma comunicação entre vários aplicativos de *software* (EURO BANKING ASSOCIATION, 2016, p. 7).

Tal ideia permitirá que, por meio de um verdadeiro ecossistema, um cliente, se utilizando de um único provedor, acesse a todas as contas que possui, mesmo que estejam vinculadas a diferentes instituições financeiras (GAMBLIN; JONES; WILLIAMS, 2018, p. 71).

Para que isso funcione, não se tem dúvidas de que os próprios clientes deverão autorizar o uso de seus dados. Como contrapartida, pode-se falar que um usuário dos serviços terá mais facilidades, por exemplo, de cotar um empréstimo em vários bancos diversos e, a partir dali, escolher a proposta que melhor lhe antende (CUNHA, 2017)

Da mesma forma, até para evitar os riscos naturais nas operações de tratamento de dados, o *open banking* exigirá com que os *players* do setor financeiro atuem com uma maior cautela e desenvolvam melhores meios de evitar o vazamento de dados.

Por óbvio, todas as medidas que impeçam uma possível punição em duplicidade são válidas, contudo, não há notícias acerca de um acordo de cooperação entre o Banco Central e a Autoridade Nacional de Proteção da Dados.

Por esse motivo, não há como se olvidar que permanece presente o risco de que uma instituição financeira, em caso de vazamento de dados ou na hipótese de uma utilização sem autorização de tais bens, seja punida em duas esferas administrativas diversas em razão de um mesmo fato, o que, sob pena de incursão no citado *bis in idem*, não poderia ocorrer.

3.6 Conflito de atribuições junto às entidades de saúde

Da mesma forma do que ocorre nos setores já abordados, há que se abordar que nas situações que envolvem saúde, também, existe uma grande gama de dados pessoais envolvidos.

E nem poderia ser diferente, porquanto, para fins de que seja prestado qualquer atendimento, informações sobre um determinado sujeito são necessárias. Neste sentido

Nesse sentido, há que se indicar, exemplificadamente, uma alergia a um determinado medicamento, o próprio uso de remédios, preferências pessoais com relação a um procedimento mais invasivo ou não, relações familiares, dentre outras diversas circunstâncias.

Nessa perspectiva, é que, mesmo antes da Lei Geral de Proteção de Dados Pessoais, a Agência Nacional de Saúde e o próprio Conselho Federal de Medicina tratavam da temática em certa medida.

Destarte, faz-se *mister* que, também, sejam abordadas as atividades prestadas pelas entidades do ramo da saúde para que se evite uma dupla penalização de empresas que atuem

no setor.

3.6.1 *As atividades das entidades de saúde*

O setor de saúde, em razão da importância de tal bem jurídico, é controlado por diversas entidades de âmbito administrativo.

Diz-se isso, pois para cada um dos ângulos daquele setor existe uma figura responsável por expedir regulamentos e outros atos que visam evitar com que a busca pelo lucro atente contra direitos fundamentais dos cidadãos.

Assim, nos termos da Lei n. 9.656/98, tem-se a Agência Nacional de Saúde regulando os planos de saúde privados. A referida agência reguladora, conforme dispõe a Lei n. 9.961/2000, possui as atribuições de propor políticas e diretrizes gerais para a regulação da saúde, estabelecer características gerais dos instrumentos contratuais do setor, elaborar rol básico de procedimentos e eventos em saúde, estabelecer critérios de credenciamento e descredenciamento das operadoras, dentre outros pontos.

Com relação às atribuições da Agência Nacional de Saúde que envolvam proteção de dados, há que se citar a integração de informações com os bancos de dados do Sistema Único de Saúde.

É dizer, a agência reguladora em comento realiza o tratamento e transferência de dados dos usuários de serviços de seguro de saúde, dados estes que, nos contornos delineados pela Lei Geral de Proteção de Dados Pessoais, são considerados sensíveis.

Considerando tal atribuição, por certo, é que a autarquia especial, há um longo tempo, já vem discorrendo acerca da temática e, por isso, deverá ajustar algumas questões com relação à Autoridade Nacional de Proteção de Dados.

Em sentido similar, faz-se *mister* suscitar que o Conselho Nacional de Medicina, autarquia federal, detém, como indicado na Lei n. 3.268/57, as atribuições de "zelar e trabalhar por todos os meios ao seu alcance, pelo perfeito desempenho ético da medicina e pelo prestígio e bom conceito da profissão e dos que a exerçam legalmente".

Além desse objetivo amplo, é certo que a própria lei supracitada prevê atuações mais específicas àquele conselho, mormente para fins de que disponha acerca de questões administrativas internas e expeça "as instruções necessárias ao bom funcionamento dos Conselhos Regionais".

Dentre as instruçõe necessárias ao bom funcionamento dos Conselhos Regionais, por certo existem atos que discorrem a respeito de pontos que se relacionem com os dados

pessoais.

Afinal, não há como se olvidar que dados afetos à saúde possuem, em caso de comercialização, um valor quase que inestimável. E isso é de simples visualização, pois esses dados permitem que hospitais, clínicas, empresas farmacêuticas e outras empresas da saúde, possam, ainda sob a premissa de *profiling* já suscitada, oferecer bens e serviços a diversos usuários da rede mundial de computadores.

Exatamente por essa razão é que, como se verá a seguir, existem pontos de intersecção entre as entidades de saúde aqui citadas e a Autoridade Nacional de Proteção de Dados.

3.6.2 *Pontos de convergência entre as atribuições dos órgãos de saúde e da Autoridade Nacional de Proteção de Dados*

Como mencionado, há pontos em comum entre atos administrativos editados por entidades da saúde e as atribuições que foram destinadas à Autoridade Nacional de Proteção de Dados, a quem, rememore-se, incumbe a obrigação de "zelar pela proteção de dados" em qualquer setor da economia.

Essa intersecção pode ser vista, por exemplo, nas Resoluções Normativas 117/2005 e 255/2011, da Agência Nacional de Sáude.

No primeiro ato normativo iluminado, é possível se verificar que aquela agência reguladora, por exemplo, abordava a necessidade de que um plano de saúde mantivesse em seus servidores informações cadastrais dos seus beneficiários e dependentes. Dentre tais informações, é possível se notar os seguintes dados:

> Art. 2º As operadoras de plano de assistência à saúde estão obrigadas a manter as informações cadastrais dos beneficiários, inclusive dependentes, representantes, prestadores de serviços integrantes ou não da rede credenciada ou referenciada, corretores, sócios, acionistas, administradores e demais clientes, bem como cópias dos documentos que dão suporte às referidas informações, sem prejuízo de outras exigências previstas em regulamentação específica.
> § 1º O cadastro de que trata o caput deverá conter, no mínimo, as seguintes informações:
> I – se pessoa física:
> a) nome completo;
> b) número de inscrição no Cadastro de Pessoas Físicas (CPF/MF);
> c) natureza e número do documento de identificação, nome do órgão expedidor e data de expedição ou dados do passaporte ou carteira civil, se estrangeiro;
> d) endereço completo (logradouro, complemento, bairro, código de endereçamento postal – CEP, cidade, unidade da federação), número de telefone e código DDD; e
> e) atividade principal desenvolvida.
> II – se pessoa jurídica:
> a) a denominação ou razão social;
> b) atividade principal desenvolvida;

> c) número de identificação no Cadastro Nacional de Pessoa Jurídica (CNPJ);
> d) endereço completo (logradouro, complemento, bairro, código de endereçamento postal – CEP, cidade, unidade da federação), número de telefone e código DDD;
> e) nome e qualificação dos representantes legais; e
> f) nome da(s) controladora(s), controlada(s) ou coligada(s).
> § 2º As operadoras de plano de assistência à saúde são responsáveis pela exatidão e atualização das informações cadastrais previstas no §1º.
> § 3º As operadoras de plano de assistência à saúde, sem prejuízo do disposto no §2º, poderão celebrar convênio ou contrato com instituições financeiras, ou empresas que façam a administração de banco de dados, que possuam cadastros com informações, ou informações e documentos, que atendam ao disposto neste artigo.
> § 4º A utilização do cadastro previsto no §3º fica condicionada à sua apresentação sempre que solicitado pela ANS.
> § 5º Os documentos e informações de que trata o caput, no caso de seguros ou contratos coletivos empresarial ou por adesão com prêmio ou contraprestação mensal, serão exigidos nos seguintes casos e formas:
> I – informações cadastrais: no ato da contratação, e no ato do pagamento do sinistro ou evento ou da devolução de prêmio ou contraprestação pecuniária por cancelamento quando em valor até R$ 10.000,00 (dez mil reais);
> II – cópia dos documentos e informações cadastrais:
> a) no ato do pagamento do sinistro ou evento quando em valor superior a R$ 10.000,00 (dez mil reais) e acima de 20% (vinte por cento) dos valores estabelecidos na Tabela TUNEP, aprovada pela Resolução *RDC nº17*, de 30 de março de 2000; e
> b) no ato da devolução de prêmio ou contraprestação pecuniária por cancelamento, quando em valor superior a R$ 10.000,00 (dez mil reais).
> § 6º No caso de co-seguro apenas a seguradora líder está obrigada a manter os documentos e informações de que trata este artigo.
> §7º No caso de pessoa física estrangeira, que contrate serviços prestados com razão justificável ou quando não for possível contratá-los em seu país de origem, é dispensável apresentação da informação prevista no inciso I, b do parágrafo 1º deste artigo.
> §8º No caso de comprovação de tentativa de atualização do cadastro em que não foi obtido êxito na totalidade das informações, não será considerada responsável a operadora desde que envie à ANS:
> I – o comprovante da tentativa frustrada de atualização do cadastro; e
> II – a listagem das informações que estão incompletas com referido motivo justificado.
> Art. 3º As operadoras de plano de assistência à saúde manterão registro e cópia dos documentos comprobatórios de quaisquer operações, relacionadas ou não à saúde suplementar, que realizarem, em moeda nacional ou estrangeira, bem como das transações com títulos e valores mobiliários, títulos de créditos, metais, ou qualquer ativo passível de ser convertido em dinheiro, quando o valor da operação for igual ou superior a R$ 10.000,00 (dez mil reais).
> Parágrafo único. Aplicar-se-á o disposto no caput quando, em um mesmo mês-calendário, se realizarem operações com uma mesma pessoa, conglomerado ou grupo que, em seu conjunto, ultrapassem o limite específico ora fixado.
> Art. 4º Os cadastros, registros e documentos mencionados nos arts. 2º e 3º devem ser mantidos organizados, à disposição da ANS, durante o período mínimo de cinco anos, a partir da emissão do(s) documento(s).

Ou seja, previu-se a realização de tratamento de dados pessoais de clientes, pessoas com alguma relação com esses clientes e, quando há contratação de pessoa jurídica, dos seus representantes legais. No mais, apenas se aceita o descumprimento de tal obrigação em hipóteses em que as operadoras conseguissem demonstram uma viabilidade no cumprimento dessa imposição.

Ao que tudo indica, mesmo porque na legislação protetiva de dados não há prazo específico de manutenção das informações pessoais dos administrados e apenas um indicativo de que o armazenamento de tais bens deve respeitar a finalidade proposta, a Resolução em baila não destoa da Lei Geral de Proteção de Dados e tampouco foi revogada.

Por isso, ainda é possível com que um tratador de dados que a desrespeite seja penalizado tanto no viés protetivo da Autoridade Nacional de Proteção de Dados quanto pela Agência Nacional de Saúde.

Nos mesmos contornos, é de rigor colocar que a Resolução n. 255/2011, também, atribuiu às operadoras de planos de saúde uma necessidade de que fosse apontado um responsável técnico com relação ao tratamento de dados.

Ademais, deixou claro que tal responsável deveria "zelar pela proteção do sigilo das informações assistenciais" e estabeleceu uma espécie de responsabilidade civil objetiva por parte da operadora de saúde na hipótese de vazamento de dados pessoais de clientes.

Mais uma vez, tendo em vista que a referida resolução continua em vigência, não se tem qualquer problemática com relação ao estabelecimento de uma pessoa responsável pelo tratamento de dados, mesmo porque a própria Lei Geral de Proteção de Dados Pessoais previu inteligência normativa semelhante.

Contudo, com relação à ideia de que todo vazamento de dados será passível de punição, o que pode ser extraído da resolução em pauta, há que se pontuar que pode existir uma contradição com a lei de dados.

Essa contradição apontada, é proveniente do quanto disposto pelo artigo 43 e incisos da Lei Geral de Proteção de Dados Pessoais, no qual se observam hipóteses em que não haverá punição aos agentes de dados. Ou seja, por certo a Agência Nacional de Saúde deverá reinterpretar eventuais punições a seus agentes com base nas novas premissas de proteção dos dados pessoais.

De qualquer maneira, nota-se que as problemáticas aqui situadas, assim como as diversas outras já vistas no bojo do presente trabalho, são plenamente capazes de permitir uma dupla penalização de um transgressor.

Por sua vez, já com relação ao Conselho Federal de Medicina, cabe citar que aquela autarquia trouxe a Resolução n. 1605/2000, que estabeleceu algumas especificações com relação à divulgação de dados de paciente sem autorização específica e, ainda, previu condições para que houvesse o envio do prontuário de uma determinada pessoa.

Desse modo, o que se tem é que o médico apenas poderá se utilizar do prontuário e dos dados ali contidos sem a autorização de seu paciente em situações onde estiver respondendo a

um processo com relação ao tema e desde que solicite a atribuição de segredo de justiça àqueles autos.

Acerca da matéria e já tendo em vista a Lei Geral de Proteção de Dados Pessoais, cabe mencionar que sobreveio a denominada Lei do Prontuário Eletrônico que estabeleceu, em sentido similar ao que já se mencionou, a necessidade de que os prontuários médicos digitalizados respeitem àquilo que consta na Lei Geral de Proteção de Dados Pessoais.

Ao assim indicar, por certo, a divulgação de tais documentos só poderá ocorrer nas hipóteses permitidas na lei protetiva de dados, dentre as quais, aliás, se encontra o consentimento do detentor dos dados pessoais e a utilização em processo judicial.

Ou seja, a princípio, tem-se uma unicidade com relação à inteligência da Lei Geral de Dados Pessoais, a Lei do Prontuário Eletrônico e a resolução do Conselho Federal de Medicina mencionada.

Por isso, é importante se evitar que sobrevenha *bis in idem* com relação à matéria divulgação e vazamento de prontuários médicos.

Outrossim, importa consignar que, diferentemente do que já se viu em matéria consumerista e concorrencial, não há, atualmente, notícias com relação a um acordo de cooperação técnica entre a Autoridade Nacional de Proteção de Dados e as entidades do setor da saúde.

Essa inexistência de pacto, sem sombra de dúvidas, faz com que exista uma insegurança ainda maior àquelas pessoas de todo um setor que, eventualmente, atuem em direção contrária ao que resta estabelecido na lei protetiva de dados e suas resoluções atreladas ao tema “proteção de dados pessoais”.

3.7 Conflito de atribuições junto a outras agências reguladoras

Mesmo que se tenha demonstrado de forma específica as probabilidades de uma dupla penalização de um agente que vá de encontro com a proteção de dados pessoais de seus clientes no bojo da Agência Nacional de Saúde, é cristalino que situações envolvendo outras agências reguladoras poderão dar ensejo a problemática de *bis in idem*.

Tal afirmativa encontra respaldo na ideia de que tais autarquias em regime especial, também, disporão de competência para que, ainda que em um nicho específico, discorram com relação à proteção de dados pessoais.

Dessa forma, cabe aqui, também, fazer um paralelo geral entre as atividades exercidas por aquelas pessoas jurídicas de Direito Público e a Autoridade Nacional de Proteção de

Dados.

3.7.1 *As atividades das agências reguladoras*

Após uma reforma no aparato do Estado brasileiro, houve uma espécie de importação de ideias surgidas nos Estados Unidos relacionadas a um acompanhamento de setores da economia por meio de Agências Reguladoras, de modo que, ao invés mater-se uma atuação direta na economia, deu-se independência a algumas entidades que deveriam controlar determinadas áreas empresariais (MONTEIRO; ROSILHO, 2017, p. 18).

Destarte, em especial nos anos 90, verificou-se uma migração do Estado de uma condição de produtor direto de bens e serviços à sociedade para uma função que envolvia uma fiscalização, incentivo e planejamento (BRESSER PEREIRA, 1998, p. 23).

Essa migração, fez com que surgissem a Agência Nacional de Energia Elétrica (ANEEL), a Agência Nacional de Telecomunicações (ANATEL), a Agência Nacional do Petróleo (ANP), a Agência Nacional de Saúde Suplementar (ANS), a Agência Nacional de Vigilância Sanitária (ANVISA), a Agência Nacional de Águas (ANA), a Agência Nacional de Transportes Aquaviários (ANTAQ), a Agência Nacional de Transportes Terrestres (ANTT), a Agência Nacional de Cinema (ANCINE) e a Agência Nacional de Aviação Civil (ANAC).

Todas as entidades em questão, as quais devem atuar com neutralidade e independência junto ao governo, possuem poderes de regulamentar as áreas técnicas em que se encontram e, conseguintemente, detém a prerrogativa de, em pontos específicos, discorrerem acerca de proteção de dados pessoais.

No mesmo contexto, é certo que eventual descumprimento de atos administrativos regulamentares de proteção de dados pessoais provenientes das agências acima poderão ser punidos por meio de processo administrativo que ali tramitem.

Por essa razão, faz-se *mister* com que tais figuras atuem de forma coordenada junto à Autoridade Nacional de Proteção de Dados, mormente para que se evite uma penalização dupla com base em um mesmo fato.

3.7.2 *Pontos de convergência entre as atribuições das agências reguladoras e da Autoridade Nacional de Proteção de Dados*

Por evidente, todas empresas pertencentes aos setores regulados pelas agências reguladoras mencionadas mais acima realizam o tratamento de dados pessoais de seus clientes.

E isso é palpável à medida em que se observa, por exemplo, que as companhias aéreas, até mesmo buscando minorar os riscos de sua atividade e informar a localização de quem adquire passagens, devem possuir os dados pessoais de seus clientes.

Esses motivos fazem com que as agências reguladoras possam e devam atuar no intuito de minorar o risco de vazamento de informações pessoais dos administrados que se utilizem dos serviços encontrados dentro de seu nicho de atuação.

É por essa razão, aliás, que a Agência Nacional de Aviação Civil editou a Instrução Normativa n. 172/2021 com o fito de aprovar a política de proteção de dados pessoais (BRASIL, 2021). Em sentido similar, tem-se que a Agência Nacional de Telecomunicações, por meio da sua Resolução Interna n. 24, também já estabeleceu pontos para se permitir um bom uso de dados no setor de telefonia (BRASIL, 2021). Ou seja, a ideia é que, até mesmo buscando se enquadrar nos termos da Lei Geral de Proteção de Dados Pessoais, todas as agências reguladoras expeçam normas similares que permitam trazer uma maior segurança aos usuários de serviços que são por ela controlados.

A maior preocupação neste ponto é que, a título ilustrativo proveniente dos atos administrativos supracitados, existem inteligências normativa no sentido de que o "descumprimento das disposições constantes nesta Política e nas normas complementares sobre proteção de dados pessoais caracteriza violação de dever funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades civil e penal" e a "Anatel estabelecerá, em normativo próprio, o procedimento relativo à gestão de incidentes de dados pessoais".

Isso significa que, no próprio bojo das agências reguladoras, poderá se ter procedimentos administrativos que visem apurar vazamento de dados e que, ao final, trarão penalidades aos controladores e operadores de dados.

Nesse cenário, é inconteste que, ainda, falta uma coordenação efetiva em âmbito federal e, por essa razão, é plenamente possível que, em nichos da economia em que atuem autarquias especiais, exista um *bis in idem*.

Feitas tais colocações, é notório que a questão problemática está, apesar de esforços dispensados, longe de finalizar.

CONCLUSÃO

É possível se afirmar que, atualmente, subsiste uma grande probabilidade de que uma determinada empresa que realize o tratamento de dados de forma dissonante ao que prevê a Lei Geral de Proteção de Dados Pessoais seja punida por diversas vias de âmbito administrativo.

Isso porque, existem setores de mercado que, dada a sua importância, já receberam do legislador figuras reguladoras que, dentre outros temas e em certa medida, já expediram atos administrativos que englobam, ainda que de forma indireta, o tratamento de informações de cidadãos usuários de bens e serviços disponíveis.

É o caso, como visto, de matérias de cunho consumerista, de espeque concorrencial, bancário e da área de saúde, as quais possuem entidades de controle como o Procon, o Conselho Administrativo de Defesa Econômica, o Banco Central, a Agência Nacional de Saúde, dentre outros.

Em todos os casos, é certo que já existem atos normativos provenientes das entidades supracitadas que discorrem a respeito da proteção de dados e tal circunstância torna possível com que surjam processos administrativos tanto no âmbito das referidas entidades quanto no bojo da Autoridade Nacional de Proteção de Dados.

Pode-se afirmar, desse modo, que a proteção dos dados pessoais, até mesmo em razão da sua envergadura de direito constitucional, é uma questão que é observada e controlada por diversas entidades.

Assim, não obstante caiba à Autoridade Nacional de Proteção de Dados uma guarida geral e ampla, é certo que, conforme se extrai do ordenamento jurídico pátrio em vigor, outras figuras poderão atuar com relação à temática.

Essa perspectiva de atuação simultânea e disparsa, contudo, além de atentar à ideia de cooperação contida na Lei Geral de Proteção de Dados Pessoais, vai de encontro a outro direito fundamental, qual seja, o de que o Estado deve ter limites para realizar punições aos infratores de norma, o que engloba a impossibilidade de se ter um *bis in idem*, ou seja, uma dupla penalização em razão de uma mesma conduta.

Obviamente, até mesmo em razão de conhecidas construções jurisprudencial e doutrinária, é impossível se ter uma mesma infração produzindo mais de um efeito em uma mesma seara. Em outros termos, não obstante seja possível um ato gerar uma sanção de cunho administrativo, uma de caráter penal e uma de caráter cível, não há como se ter mais de uma punição em uma mesma seara.

Com efeito, a situação problema apresentada, por trazer um *bis in idem* no sentido de que um mesmo desrespeito ao disposto na lei protetiva de dados consiste em uma afronta a outras normas e atos administrativos, deve ser evitada a todo custo.

Apesar de já se notarem tentativas de impedir que isso ocorra por meio da assinatura de acordos de cooperação mútua entre a Autoridade Nacional de Dados e outras figuras, cabe colocar que os termos são muito iniciais e, por esse motivo, completamente insuficientes para fins de atingir o escopo pretendido pelo legislador e pelos próprios envolvidos nos referidos pactos.

Outrossim, é evidente que, ainda, não foram firmados acordos de cooperação entre a Autoridade Nacional de Proteção de Dados e todas as entidades que possuem alguma relação que trate do tema.

Destarte, buscando suprir esse vácuo que subsiste, há de se realizar algumas proposições.

A primeira proposição é no sentido de, por meio de outro decreto, dar-se nova redação ao artigo 2º, do Decreto n. 2.181/1997, de modo a fazer com que a Autoridade Nacional de Proteção de Dados seja incluída como integrante do Sistema Nacional de Defesa do Consumidor.

Isso porque, tendo em vista que aquele decreto prevê uma união de órgãos federais que tenham um intuito de proteger consumidores, seria importante, até mesmo para fins de facilitar uma atuação em sincronia a diversos outros órgãos (como Procons estaduais, municipais e federal), que a Autoridade Nacional de Proteção de Dados participasse de deliberações que tenham uma busca pela melhoria na proteção de dados no âmbito daquela entidade.

Essa inclusão, sabendo-se que existe uma perspectiva de se solucionar uma discussão acerca de atribuição no bojo daquele decreto, pode fazer com que, por meio de uma outra alteração no parágrafo único do artigo 5º, seja estabelecido campo de discussão para definir sob quem recairá a responsabilidade para discutir um prisma ou outro de eventual ato atentatório da privacidade dos administrados, bem como minoraria as chances de que, paralelamente, tramitassem dois procedimentos administrativos que tratem de uma mesma situação problema.

Essas alterações normativas propostas, sem dúvidas, facilitaria o estabeleciemento de situações mais palpáveis e menos amplas que aquela disposição contida no acordo de cooperação técnica firmado entre Autoridade Nacional de Proteção de Dados e Senacon no sentido de que dever-se-ia pacificar o "endereçamento de reclamações" e, também, traria uma maior observância à ideia de cooperação vista no bojo da Lei Geral de Proteção de Dados

Pessoais.

Com relação às situações de intersecção entre atribuições do Conselho Administrativo de Defesa Econômica e a Autoridade Nacional de Proteção de Dados, cabe propor uma melhor individualização do conceito aberto que traz a ideia de "viabilizar ações a serem adotadas pelas partes, de forma conjunta e coordenada, quando da ocorrência de situações que interseccionam ambas as esferas de competências".

Portanto, ainda que se traga um rol taxativo, cumpre, desde já, esclarecer, por exemplo, se as situações relacionadas ao *profiling* que traga vantagem econômica serão cotejadas pela perspectiva de proteção de dados ou pelo viés econômico. Da mesma forma, há que se estabelecer uma autoridade neutra para analisar eventuais conflitos entre as duas entidades em pauta.

Por sua vez, com relação ao Banco Central, entidades de controle do setor de saúde e agências reguladoras, é certo que, primeiramente, a Autoridade Nacional de Proteção de Dados deve buscar acordos de cooperações técnicas.

Como esses acordos, até o momento, não existem, é possível que as problemáticas já apontadas nos acordos firmados com a Senacon e o Conselho Administrativo de Defesa Econômica sejam sanadas em seus nascimentos.

Ou seja, desde já, aqueles documentos deverão prever rols de intersecção e sobre quem caberá a análise de um ato que esteja em desacordo com as normativas que tratam da proteção de dados pessoais. Da mesma forma, é possível se esclarecer, de plano, uma figura administrativa que ficará responsável por uma análise casuística de conflito de atribuições, tal qual um conselho composto por autoridades que pertençam a ambos os signatários do pacto proposto.

Essas ideias, em conjunto, possivelmente permitirão com que a temática seja tratada com uma maior segurança jurídica, tornam mais difíceis alegações de nulidade de julgamentos administrativos e, também, facilitam com que se forme uma espécie de "posicionamento" com relação a quem poderá cotejar uma ou outra questão problemática.

Além disso, certamente, se possibilitará uma aprendizado mútuo entre diversas entidades que atuem no ramo de proteção de dados, como dito, uma área ampla e que possui diversos ângulos de análise.

REFERÊNCIAS

ABRÃO, Nelson. **Direito bancário**, 17. ed. – São Paulo: Saraiva Educação, 2018.

AKERKAR, Rajendra; HONG, Minsung. **Unlocking Value from Ubiquitous**, 14th International Conference, ICTERI, 2018, Kyiv, Ukraine, Revised Selected Papers.

ANDREZO, Andrea Fernandes; LIMA, Iran Siqueira. **Mercado financeiro**: aspectos históricos e conceituais. 2. ed. São Paulo: Thomson, 2002.

ARAGÃO, Alexandre Santos de. **Agências Reguladoras e a evolução do direito administrativo econômico**. 2 ed. Rio de Janeiro: Forense, 2004.

_____. **Curso de Direito Administrativo**. 2. ed. rev. atual. e ampl. Rio de Janeiro: Forense, 2014.

ARAÚJO, Alexandra Maria Rodrigues. As Transferências Transatlânticas de Dados Pessoais: o nível de proteção adequado depois de Schrems. **Revista Direitos Humanos e Democracia**, [S.L.], v. 5, n. 9, p. 201-236, 3 abr. 2017. Editora Unijui. Disponível em: http://dx.doi.org/10.21527/2317-5389.2017.9.201-236 . Acesso em: 25 jan. 2021.

ARAÚJO, Edmir Netto de. **Curso de direito administrativo**. 2. ed. São Paulo: Saraiva, 2006.

ASCENSÃO, José de Oliveira. **Direito civil: teoria geral**. São Paulo: Saraiva, 2010. v. 1.

ATRIBUIÇÃO. *In*: DICIO, Dicionário Online de Português. Porto: 7Graus, 2022. Disponível em: https://www.dicio.com.br/atribuicao/. Acesso em: 10 jan. 2022.

AZEVEDO, Álvaro Villaça. Ensino do direito romano no Brasil e na América Latina em geral. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 95, p. 203-215, 2000.

BANCO CENTRAL DO BRASIL, Resolução nº 4.658, de 26 de abril de 2018. **Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil**. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=%2FLists%2FNormativos%2FAttachments%2F50581%2FRes_4658_v1_O.pdf. Acesso em: 10 mai. 2021.

BANDEIRA DE MELLO, Celso Antônio. **Curso de Direito Administrativo**. 32. ed. revista e atualizada até a Emenda Constitucional 84, de 2.12.2014. São Paulo: Malheiros Editores, 2015.

BARBOSA, Rui. Juristas e Retóricos. In: **Antologia.** Seleção, prefácio e notas de Luís Viana. Rio de Janeiro: Casa de Rui Barbosa, 1953.

BARROSO, Luís Roberto. **Legitimidade democrática, Agências Reguladoras, Constituição, transformações do Estado e Legitimidade democrática**. São Paulo: Fórum e FGV, 2017.

_____. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a

construção do novo modelo. 2 ed., São Paulo: Saraiva, 2010.

BASSO, T.; MATSUNAGA, R. *et al*. Challenges on anonymity, privacy, and big data. In: IEEE. **Dependable Computing (LADC), 2016 Seventh Latin-American Symposium on**. [S.l.: s.n.], 2016. Disponível em: https://ieeexplore.ieee.org/document/7781852. Acesso em: 4 jan. 2021.

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

BIONI, Bruno Ricardo. *In* **Lei geral de proteção de dados (Lei nº 13.709/2018)**: a caminho da efetividade: contribuições para a implementação da LGPD; Ricardo Villas Bôas Cueva, Danilo Doneda, Laura Schertel Mendes, coordenadores. - 1. ed. - São Paulo : Thomson Reuters Brasil, 2020.

BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil**. Sequência: Estudos Jurídicos e Políticos, 2014. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109/26949. Acesso em: 28 dez. 2020.

BRASIL. ANAC. Instrução Normativa nº 172, de 2 de agosto de 2021. **Aprova a Política de Proteção de Dados Pessoais - PoPD no âmbito da Agência Nacional de Aviação Civil - ANAC**. Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/boletim-de-pessoal/2021/30s1/anexo-ii-instrucao-normativa-no-172-de-2-de-agosto-de-2021. Acesso em: 28 fev. 2022.

_____. ANATEL. Resolução Interna ANATEL nº 24, de 07 de junho de 2021. **Estabelece a Política de Proteção de Dados Pessoais da Agência Nacional de Telecomunicações**. Disponível em: https://www.telesintese.com.br/wp-content/uploads/2021/06/politica-protecao-dados-anatel-2021.pdf >. Acesso em: 28 fev. 2022.

_____. ANPD. **Acordo de Cooperação Técnica n. 1/2021**. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/arquivos/acordo_anpd_senacon_assinado.pdf. Acesso em: 4 fev. 2022.

_____. ANPD. **Acordo de Cooperação Técnica n. 5/2021**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf. Acesso em: 4 fev. 2022.

_____. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez. 2020.

_____. DPDC/Senacon, **PA n. 08012.002116/2016-21**, j. 15/06/2018, Nota Técnica n.92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ.

_____. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. **Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias**

fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www2.camara.leg.br/legin/fed/emecon/2022/emendaconstitucional-115-10-fevereiro-2022-792285-publicacaooriginal-164624-pl.html. Acesso em: 28 fev. 2022.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 out. 2020.

_____. Lei nº 12.529, de 30 de novembro de 2011. **Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica; altera a Lei nº 8.137, de 27 de dezembro de 1990, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei nº 7.347, de 24 de julho de 1985; revoga dispositivos da Lei nº 8.884, de 11 de junho de 1994, e a Lei nº 9.781, de 19 de janeiro de 1999; e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm. Acesso em: 6 fev. 2022.

_____. Lei nº 13.853, de 8 de julho de 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2. Acesso em: 3 fev. 2021.

_____. Lei Complementar nº 105, de 10 de janeiro de 2001. **Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp105.htm. Acesso em: 10 mai. 2021.

_____. Medida Provisória nº 869, de 27 de dezembro de 2018. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 out. 2020.

_____. Projeto de Lei nº 4060, de 13 de junho de 2012. **Dispõe sobre o tratamento de dados pessoais, e dá outras providências.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0yyh6kxg6cmes10qjrmh0ajcd46238068.node0?codteor=1001750&filename=PL+4060/2012. Acesso em: 3 fev. 2021.

_____. Projeto de Lei nº 5.276, de 13 de março de 2016. **Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016. Acesso em: 3 fev. 2021.

_____. Projeto de Lei nº 53, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014.** Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7738705&ts=1594012449631&disposition=inline. Acesso em: 3 fev. 2021.

_____. Projeto de Lei nº 6.291, de 11 de outubro de 2016. **Altera o Marco Civil da Internet, no sentido de proibir o compartilhamento de dados pessoais dos assinantes de aplicações de internet.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0wr8n0y8dto665heqtayp3ynj21027667.node0?codteor=1497984&filename=PL+6291/2016. Acesso em: 17 nov. 2021.

_____. Presidência da República. **Mensagem de Veto n. 451/2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 3 fev. 2021.

_____. Resolução CD/ANPD Nº 1, de 28 de outubro de 2021. **Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso em: 7 jan. 2022.

_____. Superior Tribunal de Justiça (Quinta Turma). **AgRg no RHC 136961**. Relator: Min. Reynaldo Soares da Fonseca, julgado em 15/06/2021. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2069460&num_registro=202002844693&data=20210621&peticao_numero=202100442356&formato=PDF. Acesso em: 27 jan. 2022.

_____, Superior Tribunal de Justiça (Primeira Turma). **REsp 1.087.892**. Relator: Min. Benedito Gonçalves, julgado em 22/06/2010. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=952473&num_registro=200802063680&data=20100803&formato=PDF. Acesso em: 1 fev. 2022.

_____, Superior Tribunal de Justiça (Terceira Turma). **REsp 1.037.759**. Relatora: Min. Fátima Nancy Andrighi, julgado em 23/02/2010. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=946979&num_registro=200800510315&data=20100305&formato=PDF. Acesso em: 1 de fev. 2022.

_____. Supremo Tribunal Federal (Segunda Turma). **HC 171118**. Relator: Min. Gilmar Mendes, julgado em 12/11/2019. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344022609&ext=.pdf. Acesso em: 25 jan. 2022.

_____. Supremo Tribunal Federal (Segunda Turma). **Reclamação 41557**. Relator: Min. Gilmar Mendes, julgado em 15/12/2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur441745/false. Acesso em: 13 jan. 2022.

_____. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 633.782/MG**. Relator: Min. Luiz Fux, julgado em 26/10/2020. Disponível em: http://portal.stf.jus.br/processos/downloadTexto.asp?id=5208079&ext=RTF. Acesso em: 3 jan. 2022.

BRESSER PEREIRA, Luiz Carlos. **Reforma do Estado para a cidadania**: a reforma

gerencial brasileira na perspectiva internacional. Brasília: ENAP, 1998.

CABRAL, Flávio Garcia. O princípio da boa administração pública e a LGPD (Lei 13.709/18). In **LGPD e Administração Pública**: uma análise ampla dos impactos / coordenadores Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. - 1. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

CAMARINHA, Sylvia; ESPERATO, Vivian. Transferência Internacional de Dados. In **Comentários à lei geral de proteção de dados**: Lei 13.709/2018 / Bruno Feigelson e Daniel Becker, coordenação. - 1. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

CARDOSO, André Guskow. O regime de uso e compartilhamento de dados pessoais pela Administração Pública no âmbito da LGPD. **Informativo Justen, Pereira, Oliveira e Talamini,** Curitiba, n. 163, setembro de 2020. Disponível em: https://justen.com.br/pdfs/IE163/IE163-Andre-Uso-Compart-Dados-pela-Adm-LGPD.pdf. Acesso em: 13 abr. 2021.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 28. ed. São Paulo: Atlas, 2017.

CASTELLS, Manuel. **A Sociedade em Rede**. Trad. Roneide Venâncio Majer. São Paulo: Paz e Terra, 2006.

CASTRO, Carlos Roberto Siqueira. Função normativa regulatória e o novo princípio da legalidade. In: ARAGÃO, Alexandre Santos de (Org.). **Agências reguladoras**. 2. ed. Rio de Janeiro: Forense, 2005.

CASTRO, Diana Loureiro Paiva de. **Administração Pública e tratamento de dados pessoais para pesquisa científica**, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/advocacia-publica-em-estudo/dados-pessoais-pesquisa-cientifica-15102020. Acesso em 23 jan. 2020.

CAVOUKIAN Ann. **Privacy by Design** – The 7 Foundational Principles. 2009. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em 9 de jan. 2021.

CELANO, Paula Beatriz Duarte; ESPERATO, Vivian. *In* **Comentários à lei geral de proteção de dados**. Bruno Feigelson e Daniel Becker, coordenação. - 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

CENTER, Stigler. Stigler Committee on Digital Platforms: Final Report**. Stigler Center Sitio web**, 2019**.** Disponível em: https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf. Acesso em: 7 fev. 2022.

CHAVES, Luís Fernando Prado. Comentários ao artigo 33, da LGPD. In: **LGPD: Lei Geral de Proteção de Dados comentada**. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Revista dos Tribunais, 2019.

COCA VILA, Ivó. ¿Programas de Cumplimiento como forma de autorregulação regulada? In:

SILVA SÁNCHEZ, Jesús-María; FERNÁNDEZ, Raquel (Orgs.). **Criminalidad de Empresa y Compliance.** prevención y reacciones corporativas. Barcelona: Atelier, 2013.

CONFEDERAÇÃO NACIONAL DE SAÚDE. **Código de Boas Práticas**. MENDES, Laura Schertel; DONEDA, Danilo (Coords.), 2021. Disponível em: http://www.ans.gov.br/images/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_21.pdf. Acesso em: 11 mai. 2021.

CORDEIRO, António Manuel da Rocha e Menezes. **Da boa-fé no direito civil**. 5. reimpressão. Coimbra: Almedina, 2013.

CORRÊA, Ana Carolina Mariano. **Análise do consentimento na Lei de Proteção de Dados Pessoais no Brasil e sua aplicação no mundo jurídico**. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Presbiteriana Mackenzie, São Paulo, 2019.

COSTA, Nelson Nery. **Constituição Federal anotada e explicada**. 5. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2012.

COSTA, Pedro Jorge. **A consunção no direito penal brasileiro**. Porto Alegre: SAFE, 2012.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de proteção de dados pessoais comentada**. São Paulo: Thomson Reuters Brasil, 2018.

CRETELLA JÚNIOR, J. Conflito de atribuições no direito administrativo. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 80, p. 17-33, 1 jan. 1985.

CUNHA, Davi. O que é Open Banking. **Open Banking Brasil Blog**, [S.l.], 27 set. 2017. Disponível em: https://openbankingbrasil.com.br/open-banking/introducao-ao-openbanking/. Acesso em: 10 fev. 2022.

DALCIN, E.C. **Data Quality Concepts and Techniques Applied to Taxonomic Databases**. Tese de Doutorado de Filosofia, University of Southampton. 2004. Disponível em: http://www.dalcin.org/eduardo/downloads/edalcin_thesis_submission.pdf. Acesso em: 9 jan. 2021.

DALLARI, Analluza Bolivar**. A LGPD na saúde: a MP 869/2018 e os centros de pesquisa clínica privados**. Disponível em: https://www.conjur.com.br/2019-mar-20/analluza-dallari-impacto-lgpd-centros-pesquisa-clinica. Acesso em 23 jan. 2021.

DÖHMANN, Indra Spiecker. Multi-Country - The Regulation of Commercial Profiling: A Comparative Analysis. **European Data Protection Law Review**, Lexxion, v. 2, n. 4, p. 535-554, 2016. Disponível em: https://hal.archives-ouvertes.fr/hal-01522818/document. Acesso em: 11 mai. 2021.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**, v. 12, n. 2. Joaçaba: Espaço Jurídico, 2011.

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

DOS SANTOS, Maria de Fátima Ribeiro; JÚNIOR, José Luis Andrea; ZANIN, Luciana Yoshihara Arcangelo. Atuação do CADE no controle da guerra fiscal. **Revista de Direito Econômico e Socioambiental**, v. 8, n. 1, p. 182-199, 2017.

DUHIGG, Charles; POLE, Andrew. How companies learn your secrets. **New York Times**, 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp. Acesso em: 2 fev. 2022.

DUNCAN, G. T., Keller-McNulty, S. A., and Stokes, S. L. **Disclosure risk vs. data utility**: The R-U confidentiality map, 2001. Disponível em: https://www.niss.org/sites/default/files/technicalreports/tr121.pdf. Acesso em: 29 dez. 2020.

ESTADOS UNIDOS DA AMÉRICA. United States Supreme Court. **Marbury v. Madison**, 5 U.S. 137, 1803. Disponível em: https://caselaw.findlaw.com/us-supreme-court/5/137.html Acesso em 10 jan. 2022.

ESTADOS UNIDOS DA AMÉRICA. Federal Trade Comission. **In the matter of Google/DoubleClick F.T.C F.T.C. File No. 071-0170**. Disponível em: https://www.ftc.gov/enforcement/cases-proceedings/071-0170/proposed-acquisition-hellman-friedman-capital-partners-v-lp. Acesso em: 7 fev. 2022.

EURO BANKING ASSOCIATION. Understanding the business relevance of Open APIs and Open banking for banks. **Information Paper**, EBA Working Group on Electronic Alternative Payments Version 1.0, [S.l.], may 2016. Disponível em: https://thepaypers.com/reports/reportdownload/eba-understanding-the-business-relevance-of-open-apis-and-open-banking-for-banks/cid=765184. Acesso em: 10 fev. 2022.

FARINA, E. (1996) Política industrial e política antitruste: uma proposta de conciliação. **Revista do IBRAC**, 3(8).

FÁVARO, H. T. E-commerce vs geodiscriminação: o que é geoblocking e geopricing? **Jota**, 28 abr. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/coluna-do-l-o-baptista-advogados/geoblocking-geopricing-28042018. Acesso em: 4 fev. 2022.

FEIGELSON, Bruno. Tratamento de dados pessoais pelo Poder Público. In **Comentários à lei geral de proteção de dados**: Lei 13.709/2018 / Bruno Feigelson e Daniel Becker, coordenação. - 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

FEIJÓ, Alexsandro Rahbani Aragão. A constituição brasileira de 1891 e o federalismo norteamericano. **Anais do XXI Encontro Nacional do CONPEDI. Tema: Sistema Jurídico e Direitos Fundamentais Individuais e Coletivos**, v. 6, p. 07-08, 2012. Disponível em: http://www.publicadireito.com.br/artigos/?cod=e00da03b685a0dd1. Acesso em 10 jan. 2022.

FISHER, D.; DELINE R.; CZERWINSKI M.; DRUCKER S. **Interactions with big data analytics**. Interactions 19(3):50–59, 2012. Disponível em: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/inteactions_big_data.pdf. Acesso em: 4 jan. 2021.

FLUMIGNAN, Wévertton G. G. **Responsabilidade civil dos provedores no Marco Civil da Internet (Lei n. 12.965/14)**. Dissertação de Mestrado. Faculdade de Direito, Universidade de São Paulo, 2018. Disponível em:

https://www.academia.edu/37879425/Responsabilidade_civil_dos_provedores_no_Marco_Civil_da_Internet_Lei_n_12_965_14_Civil_liability_of_providers_on_the_Brazilian_internet_law_Law_n_12_965_14_. Acesso em 9 jan. 2020.

FLUMIGNAN, Wévertton; FLUMIGNAN, Silvano. Princípios que regem o tratamento de dados no Brasil. In: **Comentários à lei geral de proteção de dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. Cíntia Rosa Pereira, coordenação. São Paulo: Almedina, 2020.

FORCENETTE, Rodrigo. **Os impactos da LGPD na área tributária**. 2020. Disponível em: https://www.conjur.com.br/2020-ago-03/rodrigo-forcenette-impactos-lgpd-area-tributaria#:~:text=Em%20raz%C3%A3o%20da%20vasta%20amplitude,os%20ramos%20do%20Direito%2C%20indistintamente.&text=VI%20%E2%80%94%20para%20o%20exerc%C3%ADcio%20regular,(Lei%20de%20Arbitragem)%22. Acesso em 23 jan. 2021.

GALVÃO, Ilmar. **Parecer: Constitucionalidade Formal dos artigos 55 e 56 do Projeto de Lei da Câmara dos Deputados (PLC) nº 53/2018 (nº 4.060, de 2012, na Câmara dos Deputados)**. 2018. Disponível em: https://www.jota.info/docs/ex-ministro-diz-que-nao-ha-vicio-de-inconstitucionalidade-na-criacao-da-anpd-31072018. Acesso em: 3 fev. 2021.

GAMBLIN, Richard; JONES, Rob; WILLIAMS, Nigel. **IBM Z Integration Guide for Hybrid Cloud and the API Economy**. New York, NY: IBM Corporation, 2018.

GARCIA ALBEIRO, Ramón. **Non bis in idem**: material y concurso de leyes penales. Barcelona: Cedecs Editorial, 1995.

GASPARINI, Diógenes. **Direito Administrativo**. 13. ed. São Paulo: Saraiva, 2008.

GIMENEZ, Gabriel Nantes. **Guia de boas práticas da Lei Geral de Proteção de Dados — LGPD**, 2020. Disponível em: https://www.conjur.com.br/2020-mai-26/gimenez-guia-boas-praticas-lgpd. Acesso em: 23 jan. 2021.

GOBBI, Henrique. **Reflexos do Direito do Consumidor na Lei Geral de Proteção de Dados.** Disponível em: https://www.conjur.com.br/2020-out-04/henrique-gobbi-reflexos-direito-consumidor-lgpd. Acesso em: 20 nov. 2020.

GOODMAN, Bryce; FLAXMAN, Seth. European Union regulations on algorithmic decision-making and a "right to explanation". **AI magazine**, v. 38, n. 3, p. 50-57, 2017. Disponível em https://arxiv.org/abs/1606.08813#:~:text=version%2C%20v3)%5D-,European%20Union%20regulations%20on%20algorithmic%20decision,and%20a%20%22right%20to%20explanation%22&text=The%20law%20will%20also%20effectively,that%20was%20made%20about%20them. Acesso em: 2 fev. 2022.

GONÇALVES, Benedito; GRILO, Renato César Guedes. **Os princípios constitucionais do direito administrativo sancionador no regime democrático da constituição de 1988**. Revista Estudos Institucionais, v. 7, n. 2, mai./ago. 2021. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/636. Acesso em: 28 jan. 2022.

GRINOVER, Ada Pellegrini; [et al]. **Código brasileiro de defesa do consumidor**: comentado pelos autores do anteprojeto. Vol. I. Direito Material. 10. ed. Revista, atualizada e reformulada. Rio de Janeiro: Forense, 2011.

GUARIENTO, Daniel C.; MARTINS, Ricardo Maffeis. **A efetividade da anonimização de dados pessoais**, 2020. Disponível em: https://migalhas.uol.com.br/coluna/impressoes-digitais/319519/a-efetividade-da-anonimizacao-de-dados-pessoais. Acesso em: 4 jan. 2021.

HERNÁNDEZ, José Manuel Lavers. **O fenômeno da captura e o Direito Brasileiro**. Disponível em: https://www.direitonet.com.br/artigos/exibir/6978/O-fenomeno-da-captura-e-o-Direito-Brasileiro. Acesso em: 16 set. 2018.

HIJMANS, Hielke. **The European Union as Guardian of Internet Privacy: True Story of Art 16 TFEU**. Bruxelas: Springer International Publishing, 2016.

HOEPMAN, Jaap-Henk. **Privacy Design Strategies (The Little Blue Book)**. Publicação independente. 2019. Disponível em: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf . Acesso em: 7 jan. 2021.

IRAMINA, Aline. RGPD V. LGPD: adoção estratégica da abordagem responsiva na elaboração da lei geral de proteção de dados do Brasil e do regulamento geral de proteção de dados da união europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, nº 2, p. 91-117, out. 2020.

JUNQUEIRA DE AZEVEDO, Antonio. Insuficiências, deficiências e desatualização do projeto de código civil na questão da boa-fé objetiva nos contratos. **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 1, n. ja/mar. 2000, p. 3-12, 2000. Disponível em: http://ead2.fgv.br/ls5/centro_rec/docs/Insuficiencias_deficiencias_e_desatualizacao.pdf. Acesso em 6 jan. 2021.

JUSTEN FILHO, Marçal. **Curso de Direito Administrativo**. Revista dos Tribunais: São Paulo, 2015.

_____. **O direito das agências reguladoras independentes**. São Paulo. Dialética, 2002.

KALYVAS, James R.; OVERLY, Michael R. **Big data: a business and legal guide**. Nova Iorque, 2015.

KOSOVSKI, Ester. Minorias e discriminação. In: SÉGUIN, Elida (Coord.). **Direito das minorias**. Rio de Janeiro, Forense, 2001.

LEAL, Ana Luíza; MELLO, Luã Maia de. Agentes de Tratamento de Dados Pessoais. In **Comentários à lei geral de proteção de dados**: Lei 13.709/2018 / Bruno Feigelson e Daniel Becker, coordenação. - 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

LEITE, Luíza. Tratamento de Dados Pessoais. In **Comentários à lei geral de proteção de dados**: Lei 13.709/2018 / Bruno Feigelson e Daniel Becker, coordenação. - 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

LEITE, Salomão George; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas, 2014.

LEÓN VILLALBA, Francisco Javier de. **Acumulación de sanciones penales y administrativas**: sentido y alcance del principio ne bis in idem. Barcelona: Bosch, 1998.

LEVIN, Alexandre. Tratamento de dados pessoais pelo Poder Público – particularidades previstas na LGPD (Lei 13.709/2018). In **LGPD e Administração Pública**: uma análise ampla dos impactos / coordenadores Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. - 1. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

LIMA, Caio César Carvalho. Comentários ao artigo 8º, da LGPD. In: **LGPD: Lei Geral de Proteção de Dados comentada**. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Revista dos Tribunais, 2019.

_____. Comentários ao artigo 10, da LGPD. In: **LGPD: Lei Geral de Proteção de Dados comentada**. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Revista dos Tribunais, 2019.

LIMA, Christina Aires Correa; BARBOSA, Júlio César Moreira. **Autoridade Nacional de Proteção de Dados precisa de independência técnica**. Disponível em: https://www.conjur.com.br/2019-abr-11/opiniao-autoridade-protecao-dados-requer-autonomia-tecnica. Acesso em: 3 fev. 2021.

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

LUHMAN, Niklas. **Confianza**. México: Antropos, 2005.

MAGALHÃES, Felipe Soares de; PESSOA, Thiago Thomaz Siuves. LGPD e legal design. In **Lei Geral de Proteção de Dados**: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] / Bernardo Menicucci Grossi (Org.) - Porto Alegre, RS: Editora Fi, 2020.

MALETIC, J.I.; MARCUS, A. Data Cleansing: Beyond Integrity Analysis. In **Proceedings of the Conference on Information Quality (IQ2000)**. Boston: Massachusetts Institute of Technology. 2000. Disponível em: https://www.yumpu.com/en/document/read/35250655/data-cleansing-beyond-integrity-analysis. Acesso em 9 jan. 2021.

MASCARENHAS, Marcella Alves. **O Princípio "Ne Bis In Idem" nos Âmbitos Material e Processual sob o Ponto de Vista do Direito Penal Interno**. Revista de direito da Unigranrio, v. 2, n. 2, 2009.

MATTA, Leandro Amaral. **Em busca da autonomia operacional do Banco Central do Brasil como instrumento de estabilidade da moeda**. 2002. Dissertação (Mestrado em Administração Pública) – Fundação Getúlio Vargas, Rio de Janeiro, 2002.

MAXIMILIANO, Carlos. **Hermenêutica e Aplicação do Direito**. 20. ed. Rio de Janeiro. Forense, 2011.

MCALLISTER, Lesley K. Regulation by Third-Party Verification. ***Boston College Law Rev.*** volume 53, 2012. Disponível em: https://lawdigitalcommons.bc.edu/bclr/vol53/iss1/1. Acesso em 3 jan. 2022.

MEDAUAR, Odete. **Direito Administrativo moderno**. 21. ed. Belo Horizonte: Fórum, 2018.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. 42. ed. São Paulo: Malheiros, 2016.

MELLO, Celso Antônio Bandeira de. **Apontamentos sobre os agentes públicos**. São Paulo: Revista dos Tribunais, 1975.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469 - 483, 2018.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, ano 20, v. 79, jul./set. 2011.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Departamento de Pós-Graduação da UnB. Brasília, 2008. Disponível em: https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf. Acesso em: 29 dez. 2020.

MENEZES, Renata Oliveira Almeida. A Lei Geral de Proteção de Dados regula o segredo médico?. **Conjur**, 2020. Disponível em: https://www.conjur.com.br/2020-out-12/direito-civil-atual-lei-geral-protecao-dados-regula-segredo-medico. Acesso em: 4 jan. 2022.

MILARÉ, Édis. **Direito do Ambiente**. 3 ed. São Paulo: Revista dos Tribunais, 2004.

MONTEIRO, J. M.; BRANCO, E. C. JR; MACHADO, J. C. **Estratégias para Proteção da Privacidade de Dados Armazenados na Nuvem**. Tópicos em Gerenciamento de Dados e Informações, 2014. Disponível em: http://www.inf.ufpr.br/sbbd-sbsc2014/sbbd/proceedings/artigos/pdfs/14.pdf. Acesso em: 4 jan. 2021.

MONTEIRO, Renato Leite; CRUZ, Sinuhe. Capítulo 8. Direitos dos titulares: fundamentos, limites e aspectos práticos. **A Lei Geral de Proteção de Dados Pessoais LGPD** [livro eletrônico]: aspectos práticos e teóricos relevantes no setor público e privado / Denise de Souza Luiz Francoski, Fernando Antônio Tasso coordenadores. - 1. ed. - São Paulo: Thomson Reuters Brasil, 2021.

MONTEIRO, Vera; ROSILHO, André. Agências reguladoras e o controle da regulação pelo Tribunal de Contas da União, in PEREIRA NETO, Caio Mário da Silva; PINHEIRO, Luís Felipe Valerim (Coords.). **Direito da Infraestrutura**: volume 2. São Paulo Saraiva, 2017.

MUÑOZ CLARES, José. **Ne bis in idem y derecho penal:** definición, patologia y contrários. Murcia: Editorial DM, 2006.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Myths and Fallacies of "Personally Identifiable Information"**. Communications of the ACM, v. 53, n. 06, June 2010. Disponível

em: www.cs.utexas.edu/~shmat/shmat_cacm10.pdf. Acesso em: 4 jan. 2021.

NUCCI, Guilherme de Souza. **Curso de direito processual penal**. 17. ed. Rio de Janeiro: Forense, 2020.

NUNES, Rizatto. **Curso de Direito do Consumidor**. São Paulo: Saraiva. 2012.

OLIVEIRA, Gustavo Justino de. Administração Pública Democrática e efetivação de direitos fundamentais. **Boletim de Direito Administrativo** [recurso eletrônico], São Paulo, v. 24, n. 8, p. 904-920, ago. 2008. Disponível em: https://www.publicacoesacademicas.uniceub.br/prisma/article/download/569/494. Acesso em: 12 abr. 2021.

OLIVEIRA, Rafael Carvalho Rezende. **Curso de direito administrativo**. 9. ed. Rio de Janeiro: Forense; MÉTODO, 2021

PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados brasileira: uma visão otimista. In **Revista do Advogado** n. 144, novembro de 2019.

PEREIRA, Alexandre Libório Dias. O responsável pelo tratamento de dados segundo o regramento europeu**.** In **Proteção de dados pessoais em perspectiva**: LGPD e P967 RGPD na ótica do direito comparado / organização de Marcos Wachowicz, Curitiba: Gedai, UFPR 2020.

PEREIRA, Flávio Henrique Unes; ALVIM, Rafael da Silva. A responsabilidade civil do Estado por danos decorrentes do tratamento de dados pessoais: um estudo de caso. In **LGPD e Administração Pública**: uma análise ampla dos impactos / coordenadores Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. - 1. ed. - São Paulo: Thomson Reuters Brasil, 2020.

_____. Autorregulação na Lei Geral de Proteção de Dados e segurança jurídica. **Conjur**, 2020. Disponível em: https://www.conjur.com.br/2020-out-27/pereira-alvim-autorregulacao-lgpd-seguranca-juridica. Acesso em: 3 jan. 2022.

PEREIRA, Flávio Henrique Unes. **Regulação, fiscalização e sanção**: fundamentos e requisitos da delegação do exercício do poder de polícia administrativa a particulares. Belo Horizonte: Fórum, 2013.

PESTANA, Márcio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)**. 2019. Disponível em https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf. Acesso em: 20 nov. 2020.

PINHEIRO, Guilherme Pereira; SOUTO, Gabriel Araújo; MORAES, Thiago Guimarães. **ANPD: uma necessidade de convergência entre CADE, Anatel e Senacon**. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/anpd-uma-necessidade-de-convergencia-entre-cade-anatel-e-senacon-20102019. Acesso em: 4 jan. 2021.

PINHEIRO, Patricia Peck. **Direito digital**. 5. ed. rev., São Paulo: Saraiva, 2013.

PORTO, Antônio José Maristello; GONÇALVES, Antônio Porto; SAMPAIO, Patrícia Regina Pinheiro. **Regulação financeira para advogados**. Rio de Janeiro: Elsevier; Ed. da FGV, 2012.

PUGLIESI, Márcio; BRANDÃO, André Martins. Uma conjectura sobre as tecnologias de Big data na Prática Jurídica. In: **Revista da Faculdade de Direito da UFMG**, n. 67, p. 453-482, 2016. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/view/1731/. Acesso em: 4 jan. 2021.

QUERALT, Joan J. **El principio non bis in idem**. Madrid: Tecnos, 1992.

RAMOS, Vânia Costa. **Ne bis in idem e União Europeia**. Coimbra: Coimbra Editora, 2009

REINALDO FILHO, Demócrito. **Lei de proteção de dados pessoais aproxima o Brasil dos países civilizados**. 2018. Disponível em: https://jus.com.br/artigos/67668/lei-deprotecao-de-dados-pessoais-aproxima-o-brasil-dos-paises-civilizados. Acesso em: 6 jan. 2021.

ROCCO, Arturo. **Opere giuridiche**. Trattado della cosa giudicata come causa di estinzione dell´a azione penale. Roma: Società Editrice del Foro Italiano, 1932. v. 2

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROHAN, Paul. **Open Banking Strategy Formation**. Los Angeles, CA: Create Space, 2017.

ROSENVALD, N. **As funções da responsabilidade civil**: a reparação e a pena civil. 3. ed. São Paulo: Saraiva, 2017.

SABOYA, Keity. **Ne bis in idem**. Rio de Janeiro: Lumen Juris, 2014

SAMPAIO, José Adércio Leite Sampaio. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1997.

SANZ MORÁN, Angel José. **El concurso de delitos**: Aspectos de política legislativa. Valladolid: Secretariado de Publicaciones da Universidad de Vallodolid, 1986.

SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. Lei geral de proteção de dados no Brasil e os possíveis impactos. In: **Revista dos Tribunais**, v. 998, 2018.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação Cível 1013189-92.2018.8.26.0003**; Relator (a): Roberto Mac Cracken; Órgão Julgador: 22ª Câmara de Direito Privado; Foro Regional III - Jabaquara - 4ª Vara Cível; Data do Julgamento: 03/10/2019; Data de Registro: 07/10/2019. Disponível em: https://esaj.tjsp.jus.br/cposg/search.do;jsessionid=67379FF99972B4AC02A4E62241BE1DFF.cposg1?conversationId=&paginaConsulta=0&cbPesquisa=NUMPROC&numeroDigitoAnoUnificado=1013189-92.2018&foroNumeroUnificado=0003&dePesquisaNuUnificado=1013189-92.2018.8.26.0003&dePesquisaNuUnificado=UNIFICADO&dePesquisa=&tipoNuProcesso=UNIFICADO#. Acesso em 9 fev. 2022.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 7. ed. São Paulo: Saraiva Educação, 2018.

SARLET, Ingo Wolfgang; FENSTERSEIFER, Tiago. **Direito constitucional ambiental**: constituição, direitos fundamentais e proteção do ambiente. 3. ed. São Paulo: Editora Revista dos Tribunais, 2013.

SARTORI, Ellen Carina Mattias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet. In: **Revista de Direito Civil Contemporâneo**, v. 9, 2016. Disponível em: http://ojs.direitocivilcontemporaneo.com/index.php/rdcc/article/view/172. Acesso em 9 jan. 2021.

SCHROEDER, R. **Social Theory after the Internet**. London, UCL Press, 2018. Disponível em: https://discovery.ucl.ac.uk/id/eprint/10040801/1/Social-Theory-after-the-Internet.pdf. Acesso em: 4 jan. 2021.

SCHWIND, Rafael Wallbach. LGPD, empresas estatais e sanções aplicáveis. Jota, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-empresas-estatais-sancoes-aplicaveis-24112021. Acesso em 7 jan. 2022.

SELBST, Andrew; POWLES, Julia. Meaningful information and the right to explanation. **International Data Privacy Law**, v. 7, n. 4, 2017. Disponível em: https://academic.oup.com/idpl/article/7/4/233/4762325. Acesso em: 5 fev. 2021.

SHELTON, D. *International Law and Relative Normativity*. In: EVANS, M. International Law. ***Oxford University Press***, 2010.

SILVA, Alexandre Assunção. *In*: **Sistema brasileiro de proteção e acesso a dados pessoais: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados** – Brasília: MPF, 2019. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3. Acesso em: 29 dez. 2020.

SILVA, José Afonso da. **Curso de Direito constitucional positivo**. 33 ed. São Paulo: Malheiros, 2010.

SILVA, Pablo Rodrigo Alflen da. **Inconstitucionalidade do art. 40, inciso VII, da lei de drogas por inobservância ao ne bis in idem e violação à proibição de excesso**. BDJur, Brasília, 2009.

SOLOVE, Daniel J. Privacy self-management and the consente dilemma. **Harvard law review**, v. 126, p. 1880-1903, 2013. Disponível em: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2093&context=faculty_publications. Acesso em: 7 jan. 2021.

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

SOUZA, Matheus; LOPES, Mariana Louback; MELLO, Luã Maia. **Proteção de dados e a tutela da saúde na LGPD**. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/protecao-de-dados-e-a-tutela-da-saude-na-

lgpd-24082018. Acesso em: 24 jan. 2021.

SROUR, Robert Henry. **Ética empresarial**. Rio de Janeiro: Campus, 2000.

TABACH; Danielle; Linhares, Ludmila Anaquim. Capítulo V: Transferência internacional de dados. In **Comentários à lei geral de proteção de dados**: Lei 13.709/2018. FEIGELSON, Bruno; SIQUEIRA, Antônio Henrique Albani (Coords.). São Paulo: Revista dos Tribunais, 2019.

TARTUCE, Flávio. **A "Lei da Liberdade Econômica (Lei nº 13.874/2019) e os seus principais impactos para o Direito Civil**. 2020. Disponível em: https://flaviotartuce.jusbrasil.com.br/artigos/769067146/a-lei-da-liberdade-economica-e-os-seus-principais-impactos-para-o-direito-civil-segunda-parte-mudancas-no-ambito-do-direito-contratual. Acesso em: 19 de jan. 2021.

TENE, Omer. **Privacy law's midlife crisis**: a critical assessment of the second wave of global privacy laws. Ohio State Journal, v. 74, 2013. Disponível em: https://core.ac.uk/reader/159560945. Acesso em: 4 jan. 2021.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de dados pessoais e suas repercussões no direito brasileiro**. Revista dos Tribunais: São Paulo, 2019.

TJUE, Acórdão de 6 de outubro de 2015, processo C-362/14, **Maximilian Schrems c. Data Protection Commissioner.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN. Acesso em 25 jan. 2021.

TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé na Lei Geral de Proteção de Dados**, 2020. Disponível em: https://www.conjur.com.br/2020-mar-09/direito-civil-atual-principio-boa-fe-lgpd. Acesso em: 28 dez. 2020.

UNIÃO EUROPEIA. **Data Protection Working Party**: Opinion 02/2013 on apps on smart devices. Fevereiro, 2013. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf. Acesso em 18 jan. 2021.

VAINZOF, Rony. Comentários ao artigo 4º, da LGPD. In: **LGPD: Lei Geral de Proteção de Dados comentada**. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Revista dos Tribunais, 2019.

_____. Comentários ao artigo 6º, da LGPD. In: **LGPD: Lei Geral de Proteção de Dados comentada**. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Revista dos Tribunais, 2019.

VORONOFF, Alice. **Direito administrativo sancionador no Brasil**. 2. reimpressão. Belo Horizonte: Fórum, 2018.

WACKS, Raymond. **Personal information**. Oxford: Clarendon Press, 1989.

ZAFFARONI, Eugênio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro. **Direito penal brasileiro** I. 2. ed. Rio de Janeiro: Revan, 2003.

ZANATTA, Rafael A. F. **Perfilização, Discriminação e Direitos**: Do Código de Defesa do Consumidor à Lei Geral de Proteção de dados pessoais. 2019. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/stats. Acesso em: 2 fev. 2022.

ZANATTA, Rafael A. F.; SIMÃO, Bárbara; OMS, Juliana. **Proteção de Dados Pessoais e Sistema Nacional de Defesa do Consumidor**: Análise do PLC 53/2018. jul. 2018. Disponível em: https://idec.org.br/sites/default/files/nota_para_dpdc_-_lei_de_dados_pessoais.pdf. Acesso em: 4 jan. 2022.

_____. Tutela coletiva e coletivização da proteção de dados pessoais. In: PALHARES, Felipe (Coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020.

ZUBOFF, S. Big other: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v.30, n.1, p. 75 – 89, 2015. Disponível em: https://cryptome.org/2015/07/big-other.pdf. Acesso em: 20 nov. 2020.

ZULIANI, Evandro. Arbitragem e os órgãos integrantes do Sistema Nacional de Defesa do Consumidor. **Doutrinas Essenciais de Direito do Consumidor**. v. 6. p. 987 – 1047. São Paulo: Revista dos Tribunais, abr. 2011.