



UNIVERSIDADE DE BRASÍLIA – UNB
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

**O LEGÍTIMO INTERESSE DO CONTROLADOR OU DE TERCEIRO NO
TRATAMENTO DE DADOS PESSOAIS**

ISABELA MARIA ROSAL SANTOS

BRASÍLIA

JUNHO, 2019

ISABELA MARIA ROSAL SANTOS

**O LEGÍTIMO INTERESSE DO CONTROLADOR OU DE TERCEIRO NO
TRATAMENTO DE DADOS PESSOAIS**

Monografia apresentada à Faculdade de Direito, da
Universidade de Brasília – UnB, como requisito parcial à
obtenção de diploma no Curso de Graduação em Direito.

Orientadora: Prof.^a Dr.^a LAURA SCHERTEL MENDES

Brasília

2019

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

Monografia apresentada à Faculdade de Direito, da Universidade de Brasília – UnB, como requisito parcial à obtenção de diploma no Curso de Graduação em Direito

O LEGÍTIMO INTERESSE DO CONTROLADOR OU DE TERCEIRO NO TRATAMENTO DE DADOS
PESSOAIS

ISABELA MARIA ROSAL SANTOS

Banca examinadora:

Professora orientadora: Prof.^a Dr.^a LAURA SCHERTEL MENDES

Professor: Prof. Dr. ALEXANDRE VERONESE

Professora: Prof.^a Dr.^a AMANDA FLÁVIO DE OLIVEIRA

Brasília, 24 de junho de 2019

AGRADECIMENTOS

Antes de tudo, agradeço a minha mãe, Janaína, meu maior exemplo, apoiadora, companheira e base para todos os acontecimentos da minha vida. Tudo o que sou é graças a você, obrigada por me incentivar a realizar todos os meus sonhos, mas sabendo que tenho um porto-seguro para retornar.

Agradeço também meu pai, quem acompanha os meus passos e os estimula como se fossem dele próprio. Obrigada por ser esse grande amigo sempre, sem você não teria chegado até aqui.

À minha irmã, Nina, minha melhor amiga, origem da minha paz, essencial para que todos os processos da minha vida fossem mais leves. A sua risada é o ponto forte para todas as noites de estudo. À minha família, fonte de muito amor e encorajamento. Amo muito todos vocês!

Com grande carinho, agradeço à minha orientadora, Laura, por ter me presenteado com este tema tão desafiador e acreditado no meu trabalho. Você é uma grande inspiração, trazendo imensa inteligência e ternura na mesma pessoa. Obrigada por ter possibilitado que o processo de escrita fosse uma experiência tão gostosa. Que venham muitos trabalhos dessa parceria!

Também agradeço ao professor Alexandre Veronese, sinônimo de conhecimento e carisma. Os diálogos dentro e fora de sala me impele a criar um pensamento crítico em relação a temas tão atuais. Ainda, agradeço à professora Amanda Flávio, grande inspiração acadêmica, por ter me dado o privilégio de tê-la na banca examinadora do presente trabalho.

Nas pessoas do Mauricio e Izabella, agradeço aos companheiros de trabalho, por me ensinarem tanto e por criarem uma rotina

Agradeço aos meus amigos. Aos da vida inteira e aos com que apareceram ao longo do caminho. Obrigada por serem companhia para as conversas mais bobas e para as que mais me acrescentam, sem vocês não seria nada.

Nominalmente, agradeço ao Victor, companheiro e inspiração nessa caminhada. Obrigada por tudo.

Por fim, agradeço a Deus. Obrigada por abençoar meu caminho, colocando essas pessoas incríveis na minha jornada.

Lista de Acrônimos

ANPD – Autoridade Nacional de Proteção de Dados

CDC – Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990)

FTC - *Federal Trade Commission* (“Comissão Federal de Comércio dos Estados Unidos da América”)

RGPD – Regulamento Geral sobre a Proteção de Dados

LGPD – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018)

OCDE - Organização para Cooperação e Desenvolvimento Econômico

ONU - Organização das Nações Unidas

SAL – Secretaria de Assuntos Legislativos do Ministério da Justiça

SENACON – Secretaria Nacional do Consumidor do Ministério da Justiça

TJUE – Tribunal de Justiça da União Europeia

SUMÁRIO

INTRODUÇÃO	9
CAPÍTULO 1 – PROTEÇÃO DE DADOS PESSOAIS FUNDAMENTOS E NECESSIDADE DE PROTEÇÃO.....	13
1.1. Modelos Paradigmáticos de Proteção de Dados: Europa e Estados Unidos.....	15
1.2. Sistemática da Proteção de Dados na Europa.....	17
1.2.1. <i>Necessidade de Bases Legais para o Tratamento de Dados.....</i>	<i>18</i>
CAPÍTULO 2 – O DESENVOLVIMENTO DA LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS	20
2.1. A Construção da Lei Geral de Proteção de Dados Pessoais - LGPD	21
2.2. Bases Legais Autorizativas para o Tratamento dos Dados Pessoais	22
2.3. A Previsão do Legítimo Interesse no Modelo <i>Ex Ante</i> de Proteção de Dados	27
CAPÍTULO 3 – O LEGÍTIMO INTERESSE NO TRATAMENTO DE DADOS PESSOAIS.....	29
3.1. Fundamentos e Conceito.....	29
3.2. Caracterização do Legítimo Interesse na Prática	33
3.3. Teste de Proporcionalidade e Confecção de Relatório de Impacto	37
3.4. O Legítimo Interesse e os Dados Pessoais Sensíveis.....	47
CAPÍTULO 4 – O CONCEITO DE LEGÍTIMO INTERESSE A PARTIR DE CASOS CONCRETOS.....	50
4.1. Hipóteses de Enquadramento do Legítimo Interesse.....	50
4.2. Casos Concretos.....	56
4.3. Avaliação dos Casos Concretos	61
4.3.1. <i>Direito à Liberdade de Expressão ou Direito à informação</i>	<i>61</i>
4.3.2. <i>Finalidades Históricas, Estatísticas ou Científicas</i>	<i>62</i>
4.3.3. <i>Segurança Pública</i>	<i>62</i>
4.3.4. <i>Segurança da Informação</i>	<i>63</i>
4.3.5. <i>Riscos do Negócio</i>	<i>63</i>
4.3.6. <i>Reivindicações Legais</i>	<i>64</i>
4.3.7. <i>Marketing</i>	<i>65</i>
4.3.8. <i>Demais Hipóteses.....</i>	<i>66</i>
4.3.9. <i>Outros Casos Concretos.....</i>	<i>66</i>
CONCLUSÃO.....	72
REFERÊNCIAS BIBLIOGRÁFICAS	74

RESUMO

O trabalho busca indicar quais situações efetivamente se enquadram como modalidade de legítimo interesse do controlador ou de terceiro interessado. Para tanto, analisa precedentes do Tribunal de Justiça da União Europeia. Tal estudo permitirá entender como jurisprudência sobre o tema já existente em jurisdição submetida à regra semelhante à nacional está enquadrando os casos concretos nessa base legal – legítimo interesse. Antes disso, delimita como o legítimo interesse deverá se enquadrar em situações concretas, antes da judicialização.

Palavras-chave: legítimo interesse; interesse legítimo; tratamento de dados pessoais; bases legais; RGPD; LGPD; teste de proporcionalidade; relatório de impacto.

ABSTRACT

This paper tries to determine which situations can be distinguished as legitimate interest of the data controller or third party. For that, studies the jurisprudence of the Court of Justice of the European Union. That analyses will allow the understanding of how the jurisprudence about the theme already existent in a jurisdiction with similar rules as the Brazilian is framing the specific cases in this legal basis - legitimate interest. Besides that, sets limits about how the legitimate interest should be seen in concrete cases, before the judicialization of the matter.

Key-words: legitimate interest; processing of data; legal basis; GDPR; LGPD; proportionality test; data protection impact assessment; DPIA.

INTRODUÇÃO

A LGPD inaugurou um sistema autônomo e horizontal de proteção de dados pessoais no Brasil, aplicável a todos os setores econômicos e ao setor público¹. Apesar do tema se relacionar com outras matérias, inclusive com questões sobre privacidade, há uma tendência mundial em criar regulações específicas sobre o tema devido à relevância dos dados e à necessidade de adequação protetiva para garantir o fluxo de dados na sociedade de informações contemporânea². Então, o Brasil adotou tal inclinação global quando promulgou lei geral sobre o tema que em muito se assemelha a normas já existentes de outras jurisdições.

Algumas dessas semelhanças merecem destaque como a adoção de regulação baseada em princípios³ e a adoção de mecanismo de aplicação da norma a serem utilizados por autoridade de proteção de dados – no Brasil, a ANPD. Tais previsões garantem proteção para os titulares dos dados e para o mercado ou setor públicos, agentes que farão o tratamento de tais dados⁴. Entretanto, o presente trabalho dará maior ênfase ao modelo *ex ante* de proteção de dados⁵, sistema adotado pela LGPD, em que a regra é a proibição do tratamento, mas o próprio ordenamento já cita hipóteses em que tal processamento é legitimado, enumerando as denominadas “bases legais”.

Ao se criar uma legislação prevendo hipóteses de bases legais que autorizam o tratamento de dados pessoais, assegura-se que, em situações em que não há enquadramento de alguma dessas hipóteses, o processamento não poderá ser realizado. Tal fato conjugado com o empoderamento do titular dos dados – o qual permite que o cidadão tenha controle sobre os seus dados – possibilita ambiente propício para o tratamento adequado de tais informações.

À vista disso, a LGPD prevê bases jurídicas para justificar o tratamento de dados pessoais. Uma das hipóteses previstas é a existência do “legítimo interesse” do controlador ou de terceiro interessado. Esse é um conceito jurídico indeterminado, instrumento muitas vezes utilizado para flexibilizar sistemas rígidos. No caso da legislação brasileira, acaba por

¹ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 571.

² BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. Pp. 11-12.

³ Ibid. P. 16.

⁴ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 571.

⁵ Ibid. P. 571.

compensar a figura do “consentimento”, que tem aplicação bastante dificultada pela difícil caracterização dessa hipótese, que é conceituado na lei como consentimento livre, informado e inequívoco.

Em virtude da amplitude do termo “legítimo interesse”, os agentes de tratamento de dados, o controlador e o operador, ainda estão em ambiente inseguro no que se refere a aplicação deste conceito. Tal fato se dá porque ainda não há respostas sobre como a lei brasileira será aplicada⁶. Essa indefinição também traz insegurança ao titular dos dados, porque ainda não conhece as situações em que o controlador poderá processar seus dados de maneira legítima.

Então, apesar da lei geral brasileira sobre proteção de dados pessoais prever taxativamente as bases legais que fundamentam o tratamento de tais informações, ainda há lacunas sobre como tais critérios serão interpretados e definidos na jurisdição brasileira – destaca-se a atuação da ANPD para trazer tais definições.

Dessa forma, há lógica em recorrer às previsões da RGPD e da Diretiva 95/46/CE, normas europeias já em vigência sobre o tema, que também preveem como base legal para o processamento de dados pessoais o mesmo instituto do “legítimo interesse do controlador ou terceiro interessado”. Essa é uma das características que exemplificam as semelhanças entre as normas gerais europeias e a brasileira.

Aspecto central das normas europeias e da norma brasileira, é a necessidade de realização de um “teste de proporcionalidade” ou “teste de ponderação” prévio ao próprio tratamento, oportunidade em que verificará se o legítimo interesse naquele caso concreto sobrepõe as consequências ao titular dos dados. Ainda, ambas jurisdições citam a necessidade de confecção de relatórios de impacto como forma de verificar os efeitos para o titular.

Então, é racional se voltar para a experiência europeia para verificar quais situações efetivamente já foram caracterizadas como forma de interesse legítimo de controlador ou terceiro⁷. Tais casos, ainda que relacionados à jurisdição europeia, podem auxiliar os agentes de tratamento de dados a realizar testes de proporcionalidade de forma mais completa, gerando relatórios de impactos melhores e trazendo maior segurança tanto para o controlador quanto para o titular. Nesse sentido, mesmo precedentes internacionais podem cumprir importante

⁶ NAUWELAERTS, Wim. *GDPR - The Perfect Privacy Storm: You can Run from the Regulator, but You Cannot Hide from the Consumer*. 3 Eur. Data Prot. L. Rev. 2017. pp. 251-256.

⁷ Durante o um ano de vigência da RGPD 70% dos casos de tratamento de dados pessoais foi justificado pela caracterização do legítimo interesse do controlador ou de terceiro interessado, como citado por Marcel Leonardi no *Seminário Internacional - Lei Geral de Proteção de Dados: a caminho da efetividade*, disponível em: <<https://www.youtube.com/watch?v=j8m-CB3EeTs>>. Acesso em 30/05/2019.

função para o momento inicial da aplicação da norma brasileira⁸ em que ainda não há orientações para o controlador sobre a caracterização do legítimo interesse.

Recorrer à jurisprudência estrangeira se justifica pelo fato de regulações sobre privacidade seguirem tendência de apresentar teor globalizado. Essa característica conjugada ao fato de que as normas nacionais sobre proteção de dados buscam criar instrumentos para além das fronteiras pátrias demonstra a inclinação das jurisdições em buscar uma convergência internacional⁹.

Esse movimento é marcado pela criação de critérios mínimos de proteção sobre os dados e pela previsão de instrumentos de aplicação também globalizados a fim de possibilitar a transferência internacional segura dessas informações. O objetivo é possibilitar a interoperabilidade transnacional, o que justifica a comparação de leis de diferentes jurisdições, mas que apresentam teor semelhantes¹⁰.

Por essas razões expostas, este trabalho tem objetivos semelhantes aos do Parecer 06/2014 confeccionado pelo Grupo de Trabalho do Artigo 29¹¹, que buscou aumentar a segurança jurídica e delimitar situações que já definiram limites para a utilização do legítimo interesse¹² para o tratamento de dados pessoais¹³.

Para tanto, o primeiro capítulo do trabalho buscará avaliar dois sistemas de proteção de dados pessoais paradigma para o assunto, quais sejam, o sistema europeu e o sistema norte

⁸ A LGPD entrará efetivamente em vigor em agosto de 2020, conforme disposto no artigo 65, inciso II da LGPD: “Esta Lei entra em vigor: II - vinte e quatro meses após a data de sua publicação quanto aos demais artigos”. A publicação foi feita no dia 15/08/2018.

⁹ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. Pp. 6, 12, 15 e 36.

¹⁰ *Ibid.* Pp. 6, 12, 15 e 36.

¹¹ O Grupo de Trabalho do Artigo 29 era um órgão europeu consultivo no que se trata da matéria de proteção de dados e de privacidade. Ele foi instituído pelo artigo 29 da Diretiva 95/46/CE e suas atribuições são delimitadas no artigo 30 da mesma Diretiva e no artigo 15 da Diretiva 2002/58/CE.

Após a promulgação do RGPD, o Grupo de Trabalho foi substituído pelo *European Data Protection Board* (EDPB). O EDPB é um órgão europeu independente que contribui para a uniformização da aplicação das regras sobre proteção de dados na União Europeia além de promover a cooperação entre as Autoridades de Proteção de Dados, principalmente entre os Estados-Membro. Para maiores informações, visitar o *site* da instituição, disponível em: < https://edpb.europa.eu/about-edpb/about-edpb_en>. Acesso em 11/06/2019.

¹² O Parecer 06/2014 não foi expressamente adotado pelo EDPB. Sua última revisão e adoção foi feita em 2014, ou seja, antes da vigência do RGPD. Contudo, já traz previsões sobre como este órgão - EDPB - deverá providenciar mais direcionamentos sobre a utilização da base legal legítimo interesse, como por exemplo na página 54 do Parecer: “*The Working Party considers it also advisable to entrust the EDPB with providing further guidance where necessary on the basis of this framework. This approach would allow both sufficient clarity in the text and sufficient flexibility in its implementation*”.

Tendo em vista que não há documentos do EDPB específicos sobre o tema e, considerando a relevância deste Parecer na temática, ele será considerado ao longo do presente trabalho.

¹³ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. P. 250.

americano. Com esta breve avaliação, busca-se demonstrar as semelhanças do sistema europeu com o sistema brasileiro.

No capítulo seguinte, a pesquisa passará ao estudo da legislação brasileira específica sobre o tema, a LGPD, com enfoque nas bases legais previstas na própria norma que autorizam o tratamento dos dados pessoais. A partir dessa dinâmica, pretende-se demonstrar que o “legítimo interesse do controlador ou de terceiros” é base ampla, mas importante para o sistema rígido e proibitivo brasileiro.

Em continuidade, o próximo capítulo tentará definir o legítimo interesse, caracterizando todas as variáveis previstas no inciso da normativa brasileira. Em seguida, tentar-se-á determinar a importância do “teste de proporcionalidade” para possibilitar o tratamento seguro dos dados baseados na alegação de legítimo interesse e definir como ele é essencial para a confecção dos relatórios de impacto - documentos prévios necessários para qualquer tratamento de dados baseados no legítimo interesse¹⁴.

Para todos esses passos foi feita revisão bibliográfica. Destaca-se ainda não há quantidade expressiva de materiais específicos sobre esse tema. Dessa forma, a pesquisa é feita a partir de trabalhos com enfoques distintos, tais como direito trabalhista ou direito internacional, mas que abordam de alguma maneira o conceito “legítimo interesse do controlador”.

O último capítulo do texto traz análise qualitativa de casos do Tribunal de Justiça da União Europeia sobre o tema nos últimos cinco anos. O objetivo é definir como o legítimo interesse e, conseqüentemente, o “teste de proporcionalidade”, são aplicados na prática. Essa análise permitirá confirmar se algumas hipóteses doutrinárias foram caracterizadas na prática.

Afinal, apesar da doutrina definir situações em que o interesse legítimo provavelmente irá prevalecer na ponderação com os direitos e liberdades do titular, cabe entender como as Autoridades Nacionais - agentes de extrema relevância na proteção dos dados pessoais¹⁵ - irão efetivamente aplicar tais hipóteses.

¹⁴ Conforme artigo 10, §3º da LGPD.

¹⁵ BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 13.

CAPÍTULO 1 – PROTEÇÃO DE DADOS PESSOAIS FUNDAMENTOS E NECESSIDADE DE PROTEÇÃO

O paradigma da privacidade é entendido na Era do Big Data como um direito de controle do cidadão sobre suas informações (princípio da autodeterminação)¹⁶. A autorregulação ganha importância ao considerarmos que estamos envolvidos em uma sociedade de informação - em que a acumulação e a circulação de dados cria novas dinâmicas de poder¹⁷.

A proteção de dados é um problema político relativamente novo - principalmente quando comparado ao paradigma da privacidade - que ganhou relevância com a proliferação de informações e com o julgamento da Lei do Censo na Alemanha em 1983¹⁸. O tema é questão legal a qual se relaciona com o direito à privacidade, e, igualmente tem importância para a criação de políticas públicas além da esfera legal, inclusive pela dinamicidade das tecnologias envolvidas no tratamento de dados pessoais¹⁹.

Os dados pessoais também são essenciais para o funcionamento da economia, principalmente com a possibilidade de tratamento automatizado advindo de tecnologias. Atualmente, os dados estão ligados ao uso da internet e outros meios automatizados, o que faz com que se relacionem com atividades econômicas, sociais e políticas. Os efeitos oriundos do tratamento desses dados superam as barreiras digitais e alcançam o mundo físico²⁰.

Como são tão importantes para o desenvolvimento econômico, mas o seu tratamento gera consequências também no âmbito da privacidade individual, mostra-se necessária a criação de instrumentos que equilibrem as estruturas proibitivas, as de controle e as de processamento de dados²¹.

¹⁶ LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo, SP: Editora Saraiva, 2011. Pp. 67-68.

¹⁷ RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. Pp. 24-37.

¹⁸ LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo, SP: Editora Saraiva, 2011. P. 59. “Lei do censo”, discutida no trabalho: SCHWABE, Jürgen. *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Organização e Introdução de Leonardo Martins. Tradução de Beatriz Henning, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Galdes Ferreira. Uruguay: Konrad-Adenauer-Stiftung E.V. 2005.

¹⁹ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. Pp. 1-3.

²⁰ LIMBERGER, Têmis. *Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu*. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. P. 563.

²¹ RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. Pp. 46 e 47

A partir dessa necessidade, foram criados instrumentos de proteção aos dados pessoais, leis regulatórias, por exemplo. É possível verificar que a proteção de dados pessoais é marcada por quatro gerações de normas²².

A primeira ocorreu durante a década de 70 e foi marcada pelo controle *ex ante*, sendo necessária a autorização prévia para o tratamento. O grande foco era o Estado-social com ampla participação do cidadão. A segunda foi marcada pelo fortalecimento do Direito, com proteções constitucionais aos dados pessoais, em que a privacidade era considerada maior do que os procedimentos. A terceira geração definiu a autodeterminação como ato contínuo e, nesse contexto é que foi avaliada a constitucionalidade da Lei do Censo alemã. A última geração dá ainda mais força ao indivíduo, ao mesmo tempo que retira alguns dados, os sensíveis, da sua esfera de controle²³.

Além disso, foi percebido que as ações envolvendo dados são caracterizadas por não se estabelecerem dentro das fronteiras Estaduais, logo, justifica-se uma tentativa de equilíbrio também entre as diversas legislações internacionais²⁴. Por isso, em 2009, foram firmados os “Standards Internacionais sobre Proteção de Dados Pessoais”, fortalecendo a tese da convergência internacional, que busca a aproximação das normas transnacionais²⁵, além da atuação cada vez mais ativa de organismos internacionais como OCDE e ONU²⁶.

O passo seguinte observado foi a criação de Leis Gerais, com centralização em uma única autoridade de proteção de dados, setorizando também esse tema. A autoridade

²² LIMBERGER, Têmis. *Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu*. Direito digital: direito privado e internet, 2019, defende três fases de desenvolvimento: “1ª) 1970 - primeiras legislações *Land Hass*; 2ª) Criação das Agências de Proteção de Dados - Lei Francesa, que foi a primeira experiência; 3ª a livre circulação de dados e unificação do direito comunitário”. P. 258. Adotou-se as quatro gerações por entender que elas refletem bem as três fases de desenvolvimento, além de ir um pouco além trazendo mais um marco temporal divisório. DONEDA, Danilo. *O Direito Fundamental à Proteção de Dados Pessoais. Direito digital: direito privado e internet*. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. P. 40 Bruno Ricardo Bioni, defendeu, durante o *Seminário Internacional - Lei Geral de Proteção de Dados: a caminho da efetividade*, que com normas como a LGPD já estaríamos na 6ª geração de normas, mas optou-se por seguir a divisão mais conservadora de somente quatro gerações. Disponível em: <<https://www.youtube.com/watch?v=j8m-CB3EeTs>>. Acesso em 30/05/2019.

²³ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Pp. 37 a 44

²⁴ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p 230

²⁵ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. P. 45

²⁶ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 15.

normalmente é nacional e tem variadas funções²⁷, inclusive as de auxiliar os controladores a compreender a interpretação dos conceitos da norma geral²⁸.

Apesar de vários países ainda não terem legislação específica sobre o tema, a sua relação intrínseca com a intimidade e a privacidade individual, conceitos comumente protegidos inclusive constitucionalmente, garante que alguma tutela exista sobre a proteção dos dados pessoais nas legislações nacionais²⁹.

Mas a tendência brasileira e mundial, com promulgação de normas gerais, é se aproximar de modelos que consideram a proteção de dados pessoais como matéria autônoma, inclusive devido à aproximação do tema com a economia a partir da visão de dados como bens comerciáveis³⁰, além de criar ambientes com proteções proporcionais às de outros países que se pretende facilitar a transferência de dados pessoais.

1.1. Modelos Paradigmáticos de Proteção de Dados: Europa e Estados Unidos

Dentro do contexto atual, ou seja, a quarta geração, existem dois modelos paradigmáticos de proteção distintos: o modelo europeu e o norte-americano. Esses demonstram como ordenamentos podem oferecer diferentes soluções para o tema de proteção de dados³¹.

O sistema federativo, característica do Estado norte-americano, implica que o tema seja abordado de maneira distinta em cada estado, com diferenças na aplicação em âmbito federal³². Essa particularidade dificulta a compreensão jurídica sobre o como operar nos EUA no tocante

²⁷ MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. P. 49.

²⁸ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 23.

²⁹ LIMBERGER, Têmis. Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. Pp. 259-260, o texto estabelece como problema dessa falta de segmentação das proteções, sem existência de autoridade nacional específica, uma sobrecarga do judiciário.

³⁰ Ibid. Pp. 261-262

³¹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. Pp. 221 a 223.

³² Ibid. Pp. 303-304.

Apesar da diferenciação entre os modelos, há uma tendência de aproximação entre o federativo e difuso com a lei geral europeia. Como exemplo, a Califórnia, aprovou legislação sobre específica sobre proteção de dados, mas tem aplicação restrita. Para mais, ler *A nova lei de privacidade e proteção de dados na Califórnia*, de Viviane Trojan, disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/a-nova-lei-de-privacidade-e-protacao-de-dados-na-california-ccpa-04052019>>. Acesso em 30/05/2019.

ao tratamento de dados³³. De qualquer forma, como tentativa de padronização, dentro do *right to privacy*, a doutrina criou a *informational privacy*, subdivisão que trata de dados pessoais³⁴.

Verifica-se que o ponto central da jurisdição norte-americana é relacionado ao tratamento de dados realizado pelo Poder Público. Esse aspecto é justificado pela tendência liberal estadunidense. Então, diz-se que a regulação dos EUA de proteção de dados em relação aos agentes privados adotou modelo de auto-regulação, marcado por leis difusas e setoriais, além de atribuir funções de aplicação dessa proteção ao FTC. Contudo, a tendência atual é a de aproximação do modelo da co-regulação³⁵. Este modelo prevê mais limitações à atuação pública, no que diz respeito ao âmbito federal e através de normas setoriais³⁶.

Logo, o que se depreende é que o sistema adotado pelos EUA para proteção de dados pessoais, apesar de difuso, com aplicação heterogênea em diversos âmbitos, existe e se relaciona com várias áreas como a antitruste e a constitucional, com enfoque à proteção de dados em relação ao setor público. Contudo, não há uma segmentação com criação de norma federal específica sobre o tema, o que diferencia de maneira muito evidente os sistemas europeu e o norte-americano³⁷.

Já o modelo europeu conta com legislação geral reguladora do tratamento realizado tanto por entidades privadas quanto por autoridades públicas, criando limitações para a atuação de ambos. A pesquisa dará maior enfoque a esse modelo de legislação devido à aproximação da legislação nacional - LGPD - com as previsões das normas europeias³⁸ - Diretiva 95/46/CE e RGPD - sobre a proteção de dados pessoais³⁹.

³³ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. P. 224

³⁴ *Ibid.* P. 301

³⁵ BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em "Regulation and Governance". Pp. 16-18.

³⁶ MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014. Pp. 48-54

³⁷ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. Pp. 306-307.

³⁸ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 574.

³⁹ Como a legislação europeia sobre o tema (RGPD) criou standards bastante altos em relação a proteção de dados pessoais, é tendência que outros países e empresas multinacionais busquem harmonização de suas práticas com o sistema mais rígido, ou seja, o europeu. Como visto em BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em "Regulation and Governance". P. 17: "First, the rapid diffusion of information privacy law has produced a pervasive legal-compliance culture within global companies, and in some cases forced them to harmonize their standards with the highest (and normally EU) standard".

1.2. Sistemática da Proteção de Dados na Europa

A primeira regra padronizadora da Comunidade Europeia unificada sobre a proteção de dados pessoais foi a Diretiva 95/46/CE. A partir desse regramento, o modelo europeu prevê de forma detalhada a disciplina de proteção dos dados pessoais. Contudo, a Diretiva é somente fonte que deverá ser incorporada pela legislação nacional de cada Estado-Membro⁴⁰.

Cabe ressaltar que a Diretiva surgiu quando alguns países submetidos a ela já tinham legislação sobre o assunto (por exemplo, a Alemanha), então foi necessária a adaptação das regras nacionais. Outros países não haviam promulgado nenhuma legislação sobre o tema e incorporaram a Diretiva já na sua primeira legislação (por exemplo, a Itália), utilizando, inclusive, a experiência de outros países para a criação da primeira lei nacional sobre proteção de dados⁴¹. De qualquer forma, já em 1997, todos os 18 países submetidos à Diretiva tinham a incorporado nas legislações nacionais, alcançando posição mais firme sobre proteção de dados pessoais relacionados com a proteção de direitos fundamentais do cidadão⁴².

Essa posição fica ainda mais clara quando em 2000 foi proclamada a Carta dos Direitos Fundamentais da União Europeia, documento que reafirmou a importância da proteção de dados pessoais, ao prever, no artigo 8º da Carta, esse tema como Direito Fundamental a ser fiscalizado por autoridade independente⁴³.

Após alguns anos, entrou em vigor a Diretiva 2002/58/CE, que também versa sobre a proteção e tratamento de dados pessoais, mais especificamente sobre o setor de comunicações eletrônicas, ou seja, uma norma setorial. De qualquer forma, devido a escolha pela opção legislativa internacional Diretiva, ainda se mostrava necessário que cada Estado-Membro incorporasse as previsões normativas no direito interno de cada país⁴⁴.

⁴⁰ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. Pp. 224-226.

⁴¹ Ibid. Pp. 224-226.

⁴² Ibid. Pp. 234-235

⁴³ “Artigo 8º. Proteção de dados pessoais. 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhe digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em maio de 2019. Na Convenção Europeia para os Direitos do Homem já havia previsão do direito à vida privada, tema relacionado com a proteção de dados pessoais, mas ainda não havia previsão específica sobre os dados pessoais, o que só veio ocorrer na Carta dos Direitos Fundamentais da União Europeia.

⁴⁴ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. P. 227.

Essas três normas - Diretiva 95/46/CE, Carta de Direitos Fundamentais da União Europeia e Diretiva 2002/58/CE - previam proteções mínimas a serem fornecidas pelos Estados-Membro para os dados pessoais⁴⁵.

Somente após a promulgação da RGPD⁴⁶ houve abordagem mais homogênea da proteção nacional⁴⁷ de cada Estado-Membro⁴⁸ - inclusive na aplicação e interpretação, apesar de cada um ainda ter um período para adaptação à norma. De qualquer maneira, a RGPD incorporou grande parte das previsões das antigas Diretivas, inclusive no tocante às possibilidades de tratamento de dados pessoais, como será abordado mais adiante⁴⁹.

O caráter universalista da legislação europeia sobre o tema é visto na RGPD através da previsão sobre sua eficácia extraterritorial⁵⁰. Com essa hipótese, a norma geral europeia buscou uma maneira de proteger seus cidadãos, inclusive fora dos limites territoriais, o que é de extrema importância para a regulação de meios digitais⁵¹.

Verifica-se, então, que a RGPD é o resultado de toda essa evolução legislativa europeia⁵² trazendo respostas para vários problemas observados ao longo das últimas 5 décadas.

1.2.1. Necessidade de Bases Legais para o Tratamento de Dados

Apesar de o tratamento de dados afetar a privacidade do indivíduo, o processamento também traz vantagens para os mesmos titulares dos dados, bem como é necessário para algumas soluções, inclusive econômica. Dessa forma, em que pese o modelo adotado pela

⁴⁵ Ibid. P. 227

⁴⁶ Em 2016 foi promulgada a Diretiva 2016/680/CE relativa à proteção de dados relacionada com justiça criminal e policiamento. Essa norma também influencia o tema atualmente na União Europeia, mas não é o foco do trabalho. BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P.8.

⁴⁷ Ibid. P. 12, explica: “*the GDPR can be seen as re-converging the rules interpreting the principles following twenty or more years in which Member States’ data protection had drifted somewhat apart*”

⁴⁸ A RGPD foi promulgada através técnica legislativa diferente da Diretiva no direito continental europeu. Enquanto essa estabelece regras gerais que deverão ser incorporadas independentemente por cada Estado-Membro, aquela tem eficácia plena e as jurisdições de todos os Estados-Membros já estão submetidas a ela. Como visto em (Ibid) p. 25: “*The GDPR not only revises the 1995 Data Protection Directive to produce a single harmonized regulation for the entire EU, it is also a more multi-faceted instrument*”.

⁴⁹ A legislação se difere da Diretiva no que tange a aplicação da norma, porque ela é autoaplicável. Então, apesar de cada país ter um tempo para adaptação para compatibilização com a RGPD, todos Estados-Membros estão submetidos à norma sem a discricionariedade existente na Diretiva.

⁵⁰ LIMBERGER, Têmis. *Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu*. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco, 2019, define: “[n]o tocante ao aspecto territorial, o RGPD é aplicável no âmbito da União Europeia e a outros países ainda que não comunitários; desde que, a partir de alguma relação jurídica ou comercial, afetem os dados de cidadãos ou empresa estabelecida na União Europeia”. P. 255.

⁵¹ Ibid. P. 263.

⁵² Ibid. P. 264

legislação europeia se rígido em relação às situações em que o tratamento é legitimado, o próprio regulamento já traz as situações em que o tratamento pode acontecer⁵³.

Isso porque além de preservar um direito, as normas gerais de proteção de dados pessoais também se relacionam com a livre circulação dos dados, necessária para liberdade individual e econômica⁵⁴. É necessário, dentro do contexto de agregação de valores aos dados pessoais como bens patrimoniais, permitir o fluxo de dados desde que respeite os princípios protetivos a tal processamento como o princípio da finalidade e o princípio da minimização⁵⁵.

As aqui denominadas “bases legais para o tratamento de dados pessoais” são previstas nas normas gerais sobre o tema de forma a possibilitar o processamento de dados mesmo sem o consentimento expresso do titular desses bens⁵⁶. Especificamente na Diretiva 95/46/CE são previstas as bases legais no artigo 7º: consentimento; execução de um contrato; cumprimento de obrigação legal; proteção de interesses vitais; execução de missão de interesse público; legítimo interesse do controlador ou de terceiro interessado. A RGPD incorporou as mesmas previsões.

⁵³ Ibid. P. 255

⁵⁴ Ibid. P. 254.

⁵⁵ Ibid. Pp. 262-263

⁵⁶ INTERNETLAB, Associação Internetlab de Pesquisa em Direito e Tecnologia. *O que está em jogo no debate sobre dados pessoais no Brasil: Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de dados pessoais*. São Paulo. 2016. P. 129.

CAPÍTULO 2 – O DESENVOLVIMENTO DA LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS

A Constituição brasileira prevê a proteção à privacidade (art. 5º, X), direito interligado aos dados pessoais⁵⁷. O instrumento constitucional de controle sobre dados pessoais é o *Habeas Data*. Mas apesar da previsão no texto da Carta Magna, somente em 1997 foi regulamentado tal instrumento, através da Lei nº 9.507/97⁵⁸. A partir do Código de Defesa do Consumidor⁵⁹, promulgado em 1990, a legislação brasileira iniciou o debate sobre banco de dados e cadastros detidos por empresas.

Com o passar dos anos, mais precisamente em 2011, foram sancionadas duas Leis relacionadas com a matéria de proteção de dados, quais sejam, a Lei do Cadastro Positivo⁶⁰ e a Lei de Acesso à Informação⁶¹.

Em seguida, no ano de 2014, foi sancionado o Marco Civil da Internet⁶², que definiu a proteção de dados pessoais como princípio do uso da internet no Brasil no seu artigo 3º, inciso III⁶³. Por isso, a lei traz algumas previsões sobre a proteção de tais informações, mas ainda não pôde ser considerada como uma norma geral da proteção de dados pessoais.

Somente em 2018 foi editada a Lei nº 13.709/2018, comumente referida como Lei Geral de Proteção de Dados, que possui como objetivos proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, como previsto em seu artigo 1º⁶⁴. A lei inovou ao trazer aplicação horizontal ao setor privado e ao setor público

⁵⁷ Além disso, como visto em (LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo, SP: Editora Saraiva, 2011. P. 70) a CF também protege genericamente o sigilo de dados ao falar sobre a inviolabilidade das comunicações em seu artigo 5º, inciso XII.

⁵⁸ DONEDA, Danilo. *O Direito Fundamental à Proteção de Dados Pessoais. Direito digital: direito privado e internet*. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. Pp.48-49

⁵⁹ Lei nº 8.078, de 11 de setembro de 1990, disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078.htm>. Acesso em maio de 2019.

⁶⁰ Lei nº 12.414/11, de 9 de junho de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm>. Acesso em 30/05/2019.

⁶¹ Lei nº 12.527/1, de 18 de novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm>. Acesso em 30/05/2019.

DONEDA, Danilo. *O Direito Fundamental à Proteção de Dados Pessoais. Direito digital: direito privado e internet*. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. Pp 48-49

⁶² Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em maio de 2019.

⁶³ LIMBERGER, Têmis. *Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu*. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. P. 257.

⁶⁴ DONEDA, Danilo. *O Direito Fundamental à Proteção de Dados Pessoais. Direito digital: direito privado e internet*. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. P. 52

além de assumir um modelo *ex ante* de proteção de dados⁶⁵. Essa é a principal forma de proteção autônoma de dados pessoais na legislação nacional, com muitas semelhanças em relação a RGPD⁶⁶, e será objeto de análise deste trabalho.

2.1. A Construção da Lei Geral de Proteção de Dados Pessoais - LGPD

A LGPD é marco normativo brasileiro em matéria de proteção de dados. Inovou ao legislar horizontalmente, trazendo previsões que geram segurança ao cidadão, mas oferece, simultaneamente, mecanismos que possibilitam o fluxo informacional. Apresenta as características vistas em Leis gerais, porque é aplicável a todos os ambientes de tratamento de dados, independentemente de quem o realiza - se o setor público ou o setor privado⁶⁷.

A Lei geral brasileira foi promulgada após ao menos oito anos de debates, seminários, reuniões intersetoriais e duas consultas públicas - uma em 2010 e outra em 2015.⁶⁸ Esses debates possibilitaram a confecção do texto da LGPD, aprovado por unanimidade no Congresso Nacional⁶⁹, que contou com ativa participação opinativa de diversos agentes da sociedade.

Destaca-se a Consulta Pública realizada pela SENACON em conjunto com a SAL, em 2015, através de projeto desenvolvido pelo Ministério da Justiça. A Consulta contou com a participação de representantes do setor público e do privado, da academia, da sociedade civil e de Organizações Não-Governamentais⁷⁰.

⁶⁵ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 571.

⁶⁶ Argumenta-se que uma das justificativas para as semelhanças com o Regulamento Europeu é a adequação necessária entre legislações para possibilitar transferência de dados internacionalmente, como observado em INTERNETLAB, Associação Internetlab de Pesquisa em Direito e Tecnologia. *O que está em jogo no debate sobre dados pessoais no Brasil: Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de dados pessoais*. São Paulo. 2016. P. 13.

⁶⁷ MENDES, Laura Schertel; e DONEDA, Danilo. *Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120. 2018. Pp. 470-471.

⁶⁸ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 571.

⁶⁹ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 571.

⁷⁰ INTERNETLAB, Associação Internetlab de Pesquisa em Direito e Tecnologia. *O que está em jogo no debate sobre dados pessoais no Brasil: Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de dados pessoais*. São Paulo. 2016. P. 13

2.2. Bases Legais Autorizativas para o Tratamento dos Dados Pessoais

No Brasil, o modelo adotado para a proteção de dados se parece bastante com o modelo europeu, ao apresentar semelhanças em questões de territorialidade e a quem se aplica, nos princípios básicos, na classificação entre dados sensíveis e também no que se refere às bases legais⁷¹ que legitimam o tratamento dos dados⁷².

Durante o debate público sobre o anteprojeto da lei nacional de proteção de dados houve controvérsia entre as opiniões dos participantes sobre o alargamento ou a diminuição das bases legais para o tratamento de dados pessoais. Isso porque a redação do anteprojeto levada à debate não previa o “legítimo interesse” como base legal para o processamento dos dados. Então, adicionar essa previsão aumentaria o número de situações em que o tratamento é possibilitado, porque esse conceito amplia bastante as possibilidades de tratamento⁷³.

Após discussões, acrescentou-se previsões para o tratamento baseado no legítimo interesse e também foram adicionadas outras bases legais como o inciso sobre proteção de crédito.

A seguir, são sintetizadas as previsões legais de cada norma base para o presente estudo: a Diretiva 95/46/CE; a RGPD; e a LGPD, de forma a ilustrar as mudanças oriundas da participação de agentes de vários ramos da sociedade. O comparativo também traz a redação do anteprojeto apresentado na consulta pública. Estão destacados os excertos que preveem sobre legítimo interesse:

⁷¹ MENDES, Laura Schertel; e DONEDA, Danilo. *Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120. 2018. P. 3.

⁷² DataGuidance by Onetrust; Baptista Luz Advogados. *Comparing privacy laws: GDPR v. LGPD*. 2019

⁷³ INTERNETLAB, Associação Internetlab de Pesquisa em Direito e Tecnologia. *O que está em jogo no debate sobre dados pessoais no Brasil: Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de dados pessoais*. São Paulo. 2016. Pp. 125-130.

Tabela 1 – Comparativo entre Bases Legais para o Tratamento de Dados Pessoais

Diretiva 95/46/CE	RGPD	Anteprojeto	LGPD
Artigo 7º. Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado (sic) se:	Artigo 6º. Licitude do tratamento. 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:	Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:	Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
a) A pessoa em causa tiver dado de forma inequívoca seu consentimento;	a. O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;		I. Mediante o fornecimento de consentimento pelo titular;
b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa;	b. O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;	III - execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual o é parte o titular, observado o disposto no §1º do art. 6º;	V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito;	c. O tratamento for necessário para o cumprimento de uma obrigação jurídica que o responsável pelo tratamento esteja sujeito;	I - cumprimento de uma obrigação legal pelo responsável;	II. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa;	d. O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;	VI - proteção da vida ou da incolumidade física do titular ou de terceiro;	VII. para a proteção da vida ou da incolumidade física do titular ou de terceiro;
e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;	e. O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;	II - tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública;	III. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos

Diretiva 95/46/CE	RGPD	Anteprojeto	LGPD
			congêneres, observadas as disposições do Capítulo IV desta Lei;
f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.	f. O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.	-	IX. quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
		IV - realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;	IV. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
		V - exercício regular de direitos em processo judicial ou administrativo;	VI. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei 9.307, de 23 de setembro de 1996;
		VII - tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;	VIII. para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
		-	X. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
	O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das atribuições por via eletrônica.		

Diretiva 95/46/CE	RGPD	Anteprojeto	LGPD
		§1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.	§ 3º ⁷⁴ O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
		§2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º.	
		§3º No caso de descumprimento do disposto no §2º, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.	
			§4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
			§5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do

⁷⁴ Os parágrafos 1º e 2º da LGPD foram revogados pela Medida Provisória nº 869, de 2018. Essa foi convertida em lei no dia 08 de julho de 2019, através da sanção da Lei nº 13.853, de 08 de julho de 2019.

Diretiva 95/46/CE	RGPD	Anteprojeto	LGPD
			consentimento previstas nesta Lei.
			§6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
			§7º ⁷⁵ O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios nesta Lei.

⁷⁵ O §7º foi adicionado durante a tramitação da Lei de Conversão nº 07, de 2019, proveniente da Medida Provisória nº 869, de 2018, o qual foi sancionado através da Lei nº 13.853, de 08 de julho de 2019. Para melhor compreensão, ver o comparativo dos textos da LGPD, disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7959491&ts=1559684281528&disposition=inline>>. Acesso em 12/06/2019.

2.3. A Previsão do Legítimo Interesse no Modelo *Ex Ante* de Proteção de Dados

Diante o exposto, verifica-se que a redação da previsão do legítimo interesse na LGPD é quase idêntica ao texto da RGPD e da Diretiva 95/46/CE. Vê-se também que o legítimo interesse não era previsto originalmente na LGPD, mas a sua inclusão foi sugerida durante o Debate Público de 2015, tanto por empresas privadas⁷⁶ quanto por associações, como por exemplo a Câmara Brasileira de Comércio Eletrônico, Groupe Speciale Mobile Association, Interactive Advertising Bureau, Federação Brasileira dos Bancos, RELX Group, Centre For Information Policy Leadership e Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação. Além da inclusão, o Instituto de Tecnologia e Sociedade do Rio de Janeiro sugeriu modificação de redação que acrescentaria o legítimo interesse do responsável pelo tratamento como exceção ao consentimento⁷⁷.

Mesmo dentro desse grupo que apoiava a inclusão, foram apresentadas divergências sobre a forma da previsão. Alguns agentes, como o *Centre for Information Policy Leadership* (CIPL), falavam sobre a necessidade de que os legítimos interesses não fossem anulados por “danos ou impactos negativos” ao titular, enquanto a Brasscom, a Claro e a Vivo trouxeram sugestões menos rígidas⁷⁸.

Dessa forma e depois da devida tramitação no Congresso, da sanção e do veto do Presidente da República, foi alcançada a redação atual da Lei, afetada também pela Medida Provisória nº 869⁷⁹. Essa foi convertida na Lei nº 13.853 em 08 de julho de 2019, após sanção presidencial⁸⁰. O texto final prevê o legítimo interesse como base legal para o tratamento de dados pessoais desde que exista a comprovação de proporcionalidade entre o interesse do controlador ou de terceiros e os direitos e liberdades do titular.

Ressalta-se que a consideração de direitos e liberdades é critério mais amplo do que a análise de riscos *stricto sensu*⁸¹. Essa ponderação, necessária para o tratamento, será validada a partir da manutenção do relatório de impacto, o que será abordado adiante.

⁷⁶ As empresas Claro e Vivo.

⁷⁷ INTERNETLAB, Associação Internetlab de Pesquisa em Direito e Tecnologia. *O que está em jogo no debate sobre dados pessoais no Brasil: Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de dados pessoais*. São Paulo. 2016. Pp. 134-136

⁷⁸ Ibid. P. 135

⁷⁹ BRASIL, Medida Provisória nº 869, de 27 de dezembro de 2018. Diário Oficial da União, Brasília, 27 de dezembro de 2018.

⁸⁰ BRASIL, Lei nº 13.853, de 08 de julho de 2019. Diário Oficial da União. Brasília, 09 de julho de 2019.

⁸¹ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 33.

O legítimo interesse do controlador como base legal para o tratamento lícito de dados pessoais é apresentado desde a Diretiva de 1995⁸², foi incorporado pela RGPD e é uma das semelhanças existentes entre a lei geral europeia e a brasileira⁸³. Contudo, as normas não trazem definições sobre o que caracteriza o legítimo interesse do controlador, até porque essa caracterização depende de outros fatores a serem avaliados no caso concreto, como será abordado adiante.

Essa indefinição foi algo ponderado, como depreendido da Consulta Pública de 2015, relativa à Lei 13.709/2018⁸⁴. Isso porque o fluxo de dados na sociedade da informação é extremamente relevante e deve ser facilitado na medida do possível. Não obstante, o legítimo interesse não pode esvaziar as garantias da lei. Então, é necessário entender que não é possível restringir todas as hipóteses em que o tratamento será feito. Por isso a importância de bases abertas que respondem às inovações da sociedade, o que possibilita o fluxo de informações⁸⁵. Não obstante, os conceitos amplos como o interesse legítimo não poderão ser utilizados como um “cheque em branco ilimitado”.

Posto que o “legítimo interesse” na lei brasileira foi introduzido justamente pela previsão na legislação europeia, bem como em razão das às semelhanças de redação das duas normas, acredita-se que as situações já definidas pela União Europeia como cenários caracterizantes do legítimo interesse do controlador também serão situações em que essa base legal se caracterizará no sistema brasileiro.

⁸² O que difere a RGPD da Diretiva é a necessidade do controlador de informar, declarar, o tratamento de dados. LIMBERGER, Têmis. *Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu*. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. P. 256.

⁸³ MENDES, Laura Schertel; e DONEDA, Danilo. *Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120. 2018. P. 471.

⁸⁴ INTERNETLAB, Associação Internetlab de Pesquisa em Direito e Tecnologia. *O que está em jogo no debate sobre dados pessoais no Brasil: Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de dados pessoais*. São Paulo. 2016. Pp. 129-134

⁸⁵ BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “Regulation and Governance”. Pp. 15-16.

CAPÍTULO 3 – O LEGÍTIMO INTERESSE NO TRATAMENTO⁸⁶ DE DADOS PESSOAIS

3.1. Fundamentos e Conceito

O legítimo interesse é uma base legal aberta e flexível para o tratamento de dados. Muitas vezes os controladores ou terceiros interessados a invocam como uma forma de flexibilização⁸⁷ do sistema rígido de proteção de dados adotado tanto pela legislação brasileira quanto pela europeia⁸⁸.

Como o Direito não tem a mesma velocidade de atualização das inovações tecnológicas, é adequada a criação de um sistema rígido de proteção⁸⁹, com instrumentos de flexibilização. Objetiva-se um equilíbrio entre as estruturas proibitivas de controle, coleta e tratamento de dados e as bases legais para esses processamentos⁹⁰. Dessa forma, o que se adapta às alterações tecnológicas, sociais, culturais e contextuais é a interpretação da definição das bases que flexibilizam esse processo, tal qual o legítimo interesse⁹¹.

Por isso, a maneira de garantir a proteção de dados pessoais, conseqüentemente garantindo também a proteção de direitos fundamentais e liberdades, é partir da proibição do tratamento. Desse modo, a interferência dos controladores dos dados ou de terceiros interessados deve ser possível em determinados casos⁹², a partir de instrumentos regulatórios mais resilientes e flexíveis, mas que garantam a proteção dos direitos assegurados pelas normas sobre o tema⁹³.

⁸⁶ A LGPD, nos artigos 23 e seguintes, diferencia o tratamento de dados pessoais pelo poder público, ou seja, o tratamento a que se refere este trabalho está relacionado ao tratamento feito por entes privados.

⁸⁷ MENDES, Laura Schertel; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. P. 572.

⁸⁸ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. pp. 248 - 249

⁸⁹ BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em "Regulation and Governance". P. 5.

⁹⁰ RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Rio de Janeiro: Renovar, 2008. Pp. 41-47.

⁹¹ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. pp. 11 e 25.

⁹² *Ibid.* p. 6: "This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions". Tradução livre: "Essa abordagem é baseada em uma proibição geral de interferência no direito à privacidade e permite exceções somente em condições estritamente definidas".

⁹³ BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em "Regulation and Governance". P. 5.

Assim, o inciso IX do artigo 7 da LGPD⁹⁴ trouxe previsão legal ampla o suficiente para flexibilizar a proibição de tratamento de dados pessoais intrínseca à lei. Então, a regulação do legítimo interesse na legislação brasileira é realizada no artigo 7, inciso IX, artigo 10, e no artigo 37, conforme abaixo:

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

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

“Art. 10 O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados em seu legítimo interesse.

§3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial”

“Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse”

Para o tratamento de dados baseados no legítimo interesse do controlador ou de terceiros deverá ser feito um exame para verificar se esse interesse está em equilíbrio com as consequências para o titular dos dados. Quando existem, predominantemente, consequências ao titular, o legítimo interesse do controlador não prevalecerá. Isso porque a normativa de proteção de dados resguarda o titular dos dados ao mesmo tempo que regula as atividades dos outros agentes envolvidos nessa relação, protegendo assim um bem social⁹⁵.

Mesmo existindo como uma maneira de flexibilizar o sistema rígido, o legítimo interesse não deve ser esvaziado, o que aconteceria se fosse invocado em todos os casos de tratamento de dados. Isso aconteceria devido a sua ampla gama de aplicações que poderia anular as outras bases legais para o tratamento de dados⁹⁶. A sua invocação tampouco deve ser evitada

⁹⁴ LGPD “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”

⁹⁵ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. pp. 844-850.

⁹⁶ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* p. 5. NAUWELAERTS, Wim. *GDPR - The Perfect Privacy Storm: You can Run from the Regulator, but You Cannot Hide from the Consumer.* 3 Eur. Data Prot. L. Rev. 2017. p. 253.

devido a sua caracterização dificultada devido à previsão de necessidade de verificação de efeitos aos direitos e liberdades do titular⁹⁷.

Na mesma linha, os aplicadores das normativas não devem adicionar critérios para a definição do legítimo interesse sob pena de impedir a utilização desse fundamento legal⁹⁸. Então, os parâmetros necessários para o tratamento de dados autorizado pela base legal do artigo 7º, inciso IX da LGPD, é a caracterização do legítimo interesse e que esse interesse não ultrapasse os direitos e as liberdades fundamentais do titular.

O uso do legítimo interesse não deve ser a última categoria a ser utilizada e tampouco a preferência do controlador dos dados, mas deve ser utilizado como uma base legal para o tratamento de modo estrito e de acordo com as demais bases legais, tendo em vista que todas têm a mesma hierarquia⁹⁹.

Antes do aprofundamento sobre a caracterização do legítimo interesse do controlador ou terceiros no caso concreto, faz-se necessária uma análise dos conceitos essenciais para a interpretação do inciso IX, do artigo 7º da LGPD, quais sejam: (i) interesse; (ii) legítimo; (iii) controlador; (iv) terceiro; e (v) direitos e liberdades fundamentais do titular.

O conceito de interesse está diretamente relacionado ao princípio da finalidade, apesar deste ser mais restrito do que aquele. O princípio da finalidade no tratamento de dados pessoais é o princípio da finalidade específica (*purpose specification principle*), que prevê que os dados só poderão ser coletados para finalidades específicas, legítimas, explícitas e informadas ao titular¹⁰⁰. O conceito de “interesse” representa os benefícios que o controlador, ou terceiro, terá a partir do tratamento dos dados¹⁰¹.

O *caput* do artigo 10 da LGPD reitera que a construção do interesse deve ser baseada em situações concretas. Além de concreta, a situação deve ser atual, não podendo o enquadramento nessa base ser feito a partir de uma situação hipotética¹⁰².

⁹⁷ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. . p. 9

⁹⁸ Ibid. p. 8.

Ver também FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014, p. 863, que fala da decisão do TJUE no caso Asnef and Fecemd v. Administración del Estado (casos C-468 e C469/10), oportunidade em que a Corte reafirmou a impossibilidade de criar novas condições para caracterização do legítimo interesse, mas não fez o teste de proporcionalidade.

⁹⁹ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. pp. 9-10.

¹⁰⁰ PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. pp. 13-14.

Art. 6º, inciso I da LGPD.

¹⁰¹ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 24.

¹⁰² Ibid. P. 24-25

Além de existir o interesse do controlador ou de terceiros, é necessário que esse seja legítimo. São diversas as naturezas dos interesses que o controlador pode ter e, quanto mais clara e óbvia a demonstração de tal interesse, maior a probabilidade de enquadramento como legítimo¹⁰³.

A legitimidade pode ser bastante ampla, mas precisa não ser rechaçada pelo restante do ordenamento jurídico ao qual o sujeito está submetido¹⁰⁴. Logo, os possíveis legítimos interesses do controlador são bastante diversificados, o mais complicado é a comprovação que o caso concreto apresenta uma situação conveniente também ao titular dos dados. O importante para a caracterização da legitimidade é o objeto passar por um processo de validação e aumento de confiança¹⁰⁵.

Apesar de discursos jurídicos aproximarem a definição de legitimidade com a noção de legalidade, deve-se considerar a legitimidade no sentido amplo, ou seja, abarcando a definição social e a moral. Por exemplo, a expectativa do titular sobre o uso dos dados fornecidos ao controlador está diretamente relacionada com o conceito de legitimidade social e pode justificar o tratamento dos dados pessoais¹⁰⁶.

De qualquer forma, é importante que a legitimidade esteja de acordo com os princípios previstos na LGPD. Então, uma diferença de suma importância entre o legítimo interesse e a legalidade é a necessidade de demonstração sobre a necessidade e a proporcionalidade do tratamento de dados em detrimento dos direitos fundamentais e interesses do titular. Tais instrumentos devem ser aplicados em conjunto como forma de legitimar o processamento de dados, possibilitando a caracterização do legítimo interesse¹⁰⁷.

Já o conceito de controlador é definido na própria norma brasileira, no inciso VI do artigo 5º, que assim o define: “pessoa natural ou jurídica de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”.

A categoria “terceiro” não foi citada no rol de definições previstas no artigo 5º da LGPD, diferentemente do que foi feito no RGPD. Mas considera-se que terceiro pode ser tipificado como qualquer outra pessoa, jurídica ou natural de direito público ou privado, que poderá tratar os dados pessoais do titular, mas que não se enquadra nas categorias “controlador”¹⁰⁸,

¹⁰³ Ibid. P. 36

¹⁰⁴ Ibid. Pp. 24-25

¹⁰⁵ MAJCHER, Klaudia. *E-Commerce in the EU: Searching for Coherence of Data Protection and Competition Law in the Context of Geo-Blocking*. 24 Colum. J. Eur. L. 2018. p. 587;

¹⁰⁶ Ibid. Pp. 587-588.

¹⁰⁷ Ibid. Pp. 587-588.

¹⁰⁸ Art. 5º, inciso VI da LGPD, já citado.

“operador”¹⁰⁹, “encarregado”¹¹⁰. Porque, como há previsão expressa dessas definições, o legislador as utilizaria caso entendesse cabível na previsão do legítimo interesse. Ou seja, terceiro é uma pessoa alheia à colheita inicial dos dados pessoais, mas que pode ter acesso a eles e assim prosseguir com algum outro tipo de tratamento¹¹¹.

Os direitos e liberdades fundamentais do titular devem ser interpretados de forma abrangente como a totalidade de consequências advindas do tratamento dos dados ao titular desses¹¹². Devido ao fato de que a LGPD e a RGPD prevêm demonstração de proporcionalidade entre as categorias “legítimo interesse” e os “direitos e liberdades fundamentais” necessário que a interpretação ampla da primeira categoria e também seja utilizada nas considerações sobre a última¹¹³. Inclusive a escolha pelo termo “direitos e liberdades fundamentais” demonstra a amplitude que se deve dar ao conceito¹¹⁴.

Feita essa conceituação inicial, o trabalho passa a análise da caracterização efetiva do legítimo interesse prevista no inciso IX, art. 7º da LGPD.

3.2. Caracterização do Legítimo Interesse na Prática

A Lei brasileira optou por seguir estratégia similar à legislação europeia¹¹⁵ ao adotar uma abordagem caso-a-caso para as definições precisas sobre a caracterização do legítimo interesse. Com o julgamento de cada caso, a jurisdição brasileira fornecerá guias às empresas sobre como agir. Mas traz definições anteriores às situações concretas, porque a tentativa de

¹⁰⁹ Art. 5º, inciso VII da LGPD: “operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”.

¹¹⁰ Art. 5º, inciso VIII da LGPD: “encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados”.

O art. 5º, inciso IX da LGPD ainda prevê a definição de “agentes de tratamento” como sendo “o controlador e o operador”.

¹¹¹ O artigo 4, (10) da RGPD define “terceiro” como: “*‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who under the direct authority of the controller or processor, are authorised to process personal data*”.

¹¹² ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. pp. 30-33; 37.

¹¹³ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014 pp. 859-863.

¹¹⁴ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 33.

¹¹⁵ Tanto a Diretiva 95/46/CE quanto a RGPD.

trazer um rol taxativo¹¹⁶ de situações em que há a caracterização de legítimo interesse sem abuso dos direitos do titular seria infrutífera e contrária a própria existência dessa base legal¹¹⁷.

Dessa forma, o titular dos dados pode questionar o tratamento depois de processá-los e a empresa deverá ter provas, caso-a-caso, do enquadramento da situação na base legal “legítimo interesse”. Isso porque a primeira apreciação sobre o enquadramento do tratamento em alguma das bases legais previstas no art. 7º da LGPD é feita pelo próprio controlador, mas pode ser questionada posteriormente, caracterizando evidente inversão do ônus da prova para o controlador que será acusado no caso concreto¹¹⁸.

Nesse cenário, cabe ainda destacar que o caso de um único titular pode causar efeitos a diversos atores, então, se um titular questiona o tratamento feito com seus dados pessoais e a decisão sobre tal demonstra desproporcionalidade entre o processamento e as consequências ao titular, o controlador deverá observar os outros casos similares para se certificar que o interesse legítimo ainda está caracterizado¹¹⁹.

No Brasil, a Lei de Proteção de Dados será aplicada principalmente pela Autoridade Nacional de Proteção de Dados, mas, deve-se considerar que também servirá como base para decisões judiciais e de outros órgãos administrativos, como os organismos de defesa do consumidor¹²⁰, o que demonstra a necessidade de cooperação das autoridades nacionais que irão discutir a proteção de dados¹²¹. Em consequência disso surge a preocupação sobre a existência de uma base legal tão ampla, porque a falta de definições pode gerar desarmonia no ordenamento, o que intrinsecamente gera insegurança jurídica, tal como se observou na Europa durante a vigência da Diretiva 95/46/CE, porque cada nação aplicava o conceito de maneiras distintas¹²².

¹¹⁶ Sobre a fragilidade de criar um rol taxativo das situações que caracterizam legítimo interesse ver: FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014, p. 865, que explica que o Parlamento Europeu no debate sobre a criação da RGPD falou sobre a criação de uma lista exaustiva descrevendo quais situações o legítimo interesse do controlador supera os direitos e interesses do titular, contudo, essa ideia foi rechaçada pelo *European Data Protection Supervisor (EDPS)*, porque diminuiria a flexibilidade advinda da análise caso-a-caso.

¹¹⁷ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 12.

¹¹⁸ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 14.

¹¹⁹ NAUWELAERTS, Wim. *GDPR - The Perfect Privacy Storm: You can Run from the Regulator, but You Cannot Hide from the Consumer*. 3 Eur. Data Prot. L. Rev. 2017. p.255

¹²⁰ O art. 18, §8º da LGPD prevê: “O direito a que refere o §1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor”.

¹²¹ MAJCHER, Klaudia. *E-Commerce in the EU: Searching for Coherence of Data Protection and Competition Law in the Context of Geo-Blocking*. 24 Colum. J. Eur. L. 2018.

¹²² ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 5

Por conseguinte, essa base tão ampla justifica a importância de uma autoridade de proteção de dados, porque essa é essencial nos sistemas de proteção de dados pessoais, inclusive por trazer definições para os controladores ao passo que conscientizam ao público¹²³. É comum às leis gerais de proteção de dados a previsão de uma estrutura que busca diminuir as divergências de entendimento através de instrumentos sancionatórios e consultivos, a serem aplicados principalmente por um órgão administrativo¹²⁴, que, na LGPD, será a ANPD. Assim, o órgão será uma das fontes para definição de legítimo interesse¹²⁵

Para compreender o motivo da LGPD prever o legítimo interesse como base legal para o tratamento de dados independentemente do consentimento, deve-se entender o sistema de dados como uma “via de mão dupla”, em que o tratamento de dados muitas vezes gera benefícios tanto para o titular quanto para o controlador ou terceiro. Essa mão dupla também afeta a forma de controle nesse sistema¹²⁶. Mas, de qualquer forma, o titular ocupa uma posição de hipossuficiência¹²⁷.

Ainda há de se considerar que essa posição desprotegida pode ser agravada a depender de características do titular. Por exemplo, uma criança pode estar em uma situação de hipossuficiência extremada, e, essas características devem ser levadas em consideração. Então, o estudo caso-a caso é de extrema importância, porque quem é o titular e quem é o controlador são variáveis que importam na definição de legítimo interesse como base legal¹²⁸.

As definições dos sujeitos partem da relação analisada e também possibilitam uma melhor avaliação da expectativa do titular sobre aquele tratamento que ocorreu mesmo sem o seu consentimento. O Considerando 47¹²⁹ da RGPD prevê que o legítimo interesse pode existir

¹²³ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 13.

¹²⁴MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014. p. 49

¹²⁵ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 20.

¹²⁶ RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 46-47

¹²⁷ PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. pp. 14-15.

¹²⁸ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 37.

¹²⁹ RGPD: “(47) *The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data*

quando há uma relação entre o titular e controlador de cliente-consumidor, por exemplo¹³⁰, o que demonstra que as expectativas do titular em relação a probabilidade do tratamento podem alterar completamente a leitura sobre a situação¹³¹.

Além disso, o consentimento do titular é insuficiente para atender os interesses do controlador, porque muitas vezes não se sabe ao certo como os dados serão utilizados. Mesmo em casos em que há o consentimento, esse pode não abranger algumas finalidades supervenientes do controlador e, por isso, o tratamento de dados para a persecução dessas outras finalidades, as secundárias, seria inválido¹³².

Por isso existem bases tal qual o legítimo interesse para possibilitar o tratamento de dados¹³³ mesmo quando não há uma previsibilidade deste tratamento pelo titular, nem há relação entre a novo objetivo pretendido e a finalidade em que foi concedido o consentimento do titular¹³⁴. Um exemplo clássico de não consentimento do titular é a adição do nome do mau pagador no sistema do Serviço de Proteção ao Crédito (SPC Brasil), no sistema SERASA¹³⁵, ou em algum cadastro de negativação. Como tal categoria é negativa ao titular, esse não concederá o consentimento para que seu nome seja adicionado na lista de cadastro negativo. Mas, ao considerarmos os interesses das empresas - principalmente financeiras- é possível o tratamento de tais dados baseados no legítimo interesse desses agentes, mesmo sem a autorização do titular e ainda gerando efeitos negativos a esse¹³⁶.

controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest” (sem grifos no original)

¹³⁰ PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. p. 17-18.

¹³¹ MAJCHER, Klaudia. *E-Commerce in the EU: Searching for Coherence of Data Protection and Competition Law in the Context of Geo-Blocking*. 24 Colum. J. Eur. L.. 2018. p 592

¹³² SCHWABE, Jürgen. *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Uruguay: Konrad-Adenauer-Stiftung E.V. 2005. p. 240.

¹³³ Essa ideia é compartilhada com os controladores que participaram de pesquisa do *Centre for Information Policy Leadership an AvePoint* relatada no paper. Ver: NAUWELAERTS, Wim. *GDPR - The Perfect Privacy Storm: You can Run from the Regulator, but You Cannot Hide from the Consumer*. 3 Eur. Data Prot. L. Rev. 2017. Na página 253 explica: “*the survey suggests that a sizable portion of companies seem to think that they can easily rely on ‘legitimate interest’ as an alternative legal basis for data processing (see Graph 2). No less than 31% of the participating companies plan to make more use of legitimate interest under the GDPR than they are currently doing*”.

¹³⁴ PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. p. 13.

¹³⁵ Disponível em: <<https://www.serasaconsumidor.com.br/>>. Acesso em 17/06/2019.

¹³⁶ Como visto em MENDES, Laura Schertel; e DONEDA, Danilo. *Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120. 2018. P. 471. Esse tratamento deverá obedecer às regras das legislações específicas sobre o tema, mas também está submetido à LGPD.

Ademais, a diferença de poderes entre o titular e o controlador geram diversos problemas sobre a validade do consentimento, porque com o oferecimento de opções *take-it-or-leave-it* fica ainda mais difícil para o titular tomar decisões racionais sobre o consentimento. Tal entendimento é base para o Considerando 43 da RGPD¹³⁷ que prevê que o consentimento pode ser invalidado em situações de desequilíbrio entre o titular e o controlador¹³⁸.

A diferença entre o legítimo interesse e às demais bases legais que dispensam o consentimento é que as outras partem do pressuposto do equilíbrio dos interesses do controlador e do titular dos dados, já o legítimo interesse não pressupõe tal equilíbrio. Por essa razão, a RGPD adotou a necessidade de teste específico, com ônus da prova para o controlador ou o terceiro¹³⁹, a fim de demonstrar a caracterização do legítimo interesse¹⁴⁰, como o trabalho abordará a seguir.

Esse teste garante a verificação da existência de proporcionalidade que deve haver entre o legítimo interesse do controlador ou terceiros -inclusive àqueles que terão acesso aos dados pessoais¹⁴¹- e os direitos e liberdades fundamentais do titular¹⁴².

3.3. Teste de Proporcionalidade e Confecção de Relatório de Impacto

Mesmo após a efetiva caracterização do legítimo interesse, o Grupo de Trabalho do Artigo 29 demonstra no Parecer 06/2014 a necessidade da realização de um teste de proporcionalidade entre o “legítimo interesse” do controlador ou terceiro e os direitos e liberdades do titular. O teste foi adotado pela RGPD com previsão no próprio Artigo 6(f)¹⁴³,

¹³⁷ RGPD: “(43) *In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*”.

¹³⁸ PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. pp. 14-17.

¹³⁹ Ibid. pp. 51-53.

¹⁴⁰ Ibid. pp. 9-11.

¹⁴¹ Considerando 47 da RGPD.

¹⁴² Art. 7, inciso IX, da LGPD.

¹⁴³ Artigo 6(f) da RGPD: “*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*”.

que traz o instituto do legítimo interesse. A previsão desse teste traz segurança para essa cláusula de aplicação tão incerta¹⁴⁴.

O próprio regulamento geral europeu já cita situações em que a confecção e manutenção do relatório de impactos é obrigatória e outras em que é possível a requisição de tal documento ou situações em que a realização de tal relatório é incentivada¹⁴⁵.

Por sua vez, a norma brasileira fala sobre a necessidade da realização do teste de proporcionalidade, ao possibilitar o tratamento de dados pessoais baseados no legítimo interesse desde que direitos e liberdades fundamentais do titular não prevaleçam. Para verificação de tal teste, a legislação impõe um dever ao controlador de confecção de “relatório de impacto à proteção de dados pessoais”. Esse documento é definido no art. 5º, inciso XVII da LGPD como “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

Tal relatório poderá ser solicitado pela ANPD a qualquer momento, quando o tratamento tiver como fundamento o legítimo interesse¹⁴⁶. Então, como há grande semelhança entre a legislação brasileira e a normativa europeia, e essa adotou o teste de proporcionalidade como forma de se provar que o legítimo interesse do controlador ou do terceiro se sobrepõem às consequências ao titular¹⁴⁷, conclui-se que a única forma de explicitar esse teste de proporcionalidade é através da confecção do relatório de impactos.

O teste parte do pressuposto que não basta a caracterização do legítimo interesse, é necessária a comprovação de que o legítimo interesse, conjuntamente com os benefícios oriundos do tratamento dos dados, são maiores do que os impactos ao titular dos dados. A lei ao citar a necessidade de avaliação dos direitos e liberdades do titular interage diretamente com conceitos constitucionais bastante amplos, mais abrangentes do que a análise de riscos¹⁴⁸.

É necessária a comparação entre o legítimo interesse alegado e todas as consequências surgidas do tratamento dos dados para o titular. A interpretação desses efeitos deve ser feita da

¹⁴⁴ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. p. 845.

¹⁴⁵ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 18.

¹⁴⁶ Art, 10, §3º da LGPD: “A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial”.

¹⁴⁷ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. pp. 252-253.

¹⁴⁸ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 33.

maneira mais extensa possível. Então, em relação às consequências ao titular, deve-se analisar tanto as positivas quanto as negativas, tanto as potenciais quanto às efetivas. Essa consideração tão abrangente deve-se ao fato de que a compensação por danos na sociedade de tecnologia é difícil e, por isso, o sistema se utilizou de instrumentos preventivos¹⁴⁹.

Além disso, a previsão de balanceamento entre uma categoria ampla e sem proteção legal como o “legítimo interesse” com outra protegida constitucionalmente e internacionalmente tal como os “direitos e liberdades fundamentais do titular” pode ser incompreensível se considerarmos que os últimos são hierarquicamente superiores aos primeiros¹⁵⁰. Por isso, deve-se interpretar todas essas categorias de forma ampla para efeitos do teste de proporcionalidade.

Dois aspectos devem ser considerados para a qualificação de tais consequências, quais sejam: a probabilidade e a severidade. A probabilidade deve ser considerada de duas formas, tanto no sentido de se era provável aquele desdobramento, ou seja, se o tratamento era previsível, se o titular tinha expectativas¹⁵¹ sobre a realização daquele procedimento¹⁵², quanto no sentido de qual a chance daquele provável efeito se tornar efetivo. Como nas considerações sobre as consequências do titular até os prováveis efeitos são considerados, essa ressalva se torna importante, ao passo que quanto maior a probabilidade da concretização daquela consequência, mais peso ela agrega à balança. Sobre a severidade, ela é a base essencial para as mensurações feitas no teste, devendo ser considerada desde o número de afetados até a qualidade do risco assumido ao tratar os dados¹⁵³.

A própria legislação já trata algumas consequências severas como excludentes de proibições, como no caso de tratamento de dados pessoais sensíveis sem o fornecimento do consentimento do titular. Então, a severidade é essencial para qualificação das consequências, até porque a severidade será verificada a partir do contexto da utilização. Ou seja, dados que

¹⁴⁹ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 30-33; 37. A prevenção é princípio básico para o tratamento de dados previsto no art. 6º, inciso VIII, da LGPD.

¹⁵⁰ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. pp. 864-868. Neste trabalho o autor defende a alteração da previsão de “legítimo interesse do controlador” para “direitos do controlador” quando da criação da RGPD, porque o trabalho foi prévio a promulgação desta legislação.

¹⁵¹ NAUWELAERTS, Wim. *GDPR - The Perfect Privacy Storm: You can Run from the Regulator, but You Cannot Hide from the Consumer*. 3 Eur. Data Prot. L. Rev. 2017. p. 253. Define o legítimo interesse como um “teste de expectativas” das companhias para definir se os titulares poderiam ter a perspectiva desse processamento.

¹⁵² PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. p.17

¹⁵³ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 38.

para determinada finalidade não são significativos, para outra poderão ser considerados vulneráveis¹⁵⁴.

As consequências podem ser fonte de maiores justificativas ou motivos para interrupção do tratamento dos dados. Explico. Uma situação em que o titular corre risco de segurança, o tratamento de dados pessoais como seu endereço ou até suas senhas podem possibilitar que sua segurança seja garantida, o que pode pesar o lado da balança do legítimo interesse do controlador, mesmo considerando que o tratamento de dados como senhas têm alta probabilidade de danos severos ao titular, tornando necessárias medidas concretas tais quais modificar as senhas. Ou seja, a depender do caso, quanto maior a severidade e a probabilidade, maiores as justificativas para o tratamento ou não dos dados.

Como forma de minimizar tais efeitos, a própria LGPD já prevê só os dados “estritamente necessários para a finalidade pretendida poderão ser tratados”, ou seja, os dados a serem tratados com base no legítimo interesse serão os mínimos necessários para alcançar a finalidade pretendida. Essa previsão também esclarece a relação já mencionada do legítimo interesse com o princípio da finalidade¹⁵⁵ e também o princípio da necessidade¹⁵⁶.

Após a realização do teste, o controlador deverá manter à disposição da ANPD o relatório de impacto do tratamento realizado. Essa movimentação foi adotada pela legislação brasileira e está prevista no §3º do artigo 10 da LGPD¹⁵⁷.

É possível que mesmo após a realização do teste de proporcionalidade pelo controlador o resultado venha a ser questionado, por inúmeros motivos como por exemplo o interesse do controlador era diferente do declarado ou porque o teste não foi detalhado o suficiente, mas o objetivo do teste é minimizar os casos em que tal questionamento seja feito, gerando maior

¹⁵⁴ SCHWABE, Jürgen. *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Uruguay: Konrad-Adenauer-Stiftung E.V. 2005. p. 239.

¹⁵⁵ Sobre este princípio ler MENDES, Laura Schertel; e DONEDA, DANILO. *Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120. 2018. P. 4: “[O] exemplo do princípio da finalidade, que vincula o tratamento de dados pessoais à finalidade que motivou e justificou a sua coleta. A aplicação desse poderoso princípio tem como consequência a concretização de algumas das finalidades últimas da Lei, qual seja a consideração de que o tratamento de dados pessoais são indissociáveis de uma determinada função que sempre poderá ser avaliada, ou mesmo que dados pessoais, por estarem de certa forma ‘afetados’ por uma finalidade, jamais poderão ser considerados como mera *res in commercium*”.

¹⁵⁶ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 29.

BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P.20 avalia que a maioria dos reguladores atualmente aceita o uso de instrumentos técnicos para minimizar os impactos do tratamento aos titulares. Tais ferramentas são bastante discutidas no âmbito da *privacy by design* e se relacionam com os princípios explícitos da finalidade e necessidades e o princípio implícito da minimização.

¹⁵⁷ Art. 10, §3º “A autoridade nacional poderá solicitar ao controlador **relatório de impacto à proteção de dados pessoais**, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial” (sem grifos no original).

segurança ao titular inclusive. Por isso, o teste inicialmente será documentado pelo controlador para possíveis verificações posteriores¹⁵⁸.

O teste é uma forma de segurança para o controlador e impede o esvaziamento da base legal do legítimo interesse¹⁵⁹. Assim, em situações limítrofes, nebulosas sobre o enquadramento da situação em alguma base legal, se o resultado do teste de proporcionalidade for favorável, a adoção do legítimo interesse pode ser a melhor escolha¹⁶⁰.

Mesmo o resultado parcial do teste de proporcionalidade for desfavorável a quem deseja tratar os dados, é possível a adoção de medidas de proteção¹⁶¹ ao titular que modifiquem esse resultado preliminar¹⁶². A inexistência dessas medidas pode prejudicar a caracterização do legítimo interesse. Além disso, a existência de instrumentos eficientes e de fácil utilização pelos usuários pode alterar por completo um teste tendente a demonstrar prejuízos insuperáveis ao titular¹⁶³.

O Grupo de Trabalho do Artigo 29 define algumas medidas que podem auxiliar a justificativa para o tratamento de dados, tais como: (i) separação funcional; (ii) uso de técnicas de anonimização; (iii) agregação de dados; (iv) tecnologias para fomentar a privacidade; (v) transparência; (vi) direito de saída (*opt-out*); (vii) medidas para empoderamento do titular. A existência de alguma ou de várias dessas medidas deve ser considerada somente após a caracterização do legítimo interesse, ou seja, a existência de tais medidas não legitima qualquer interesse do controlador, sendo esta uma etapa anterior à avaliação das proteções¹⁶⁴.

Sobre a transparência (v) ressalto que a LGPD já prevê a necessidade de o controlador adotar medidas que garantam a transparência¹⁶⁵ e também consta como princípio geral para todo tipo de tratamento de dados¹⁶⁶. Os outros instrumentos são baseados nos princípios da segurança¹⁶⁷ e da não discriminação¹⁶⁸. Além disso, a normativa prevê várias dessas medidas como direitos do titular no artigo 18 do dispositivo.

¹⁵⁸ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 43.

¹⁵⁹Ibid. p. 23

¹⁶⁰Ibid. Pp. 17 e 35.

¹⁶¹ Tradução utilizada para as denominadas *safeguards*. Como sinônimo o trabalho também utiliza a expressão “salvaguarda(s)”.

¹⁶² ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. P. 34-35 e 41

¹⁶³ Ibid. p. 42.

¹⁶⁴ Ibid. p. 42

¹⁶⁵ LGPD, art. 10, §2º.

¹⁶⁶ Art. 6º, inciso VI da LGPD.

¹⁶⁷ Art. 6º, VII, da LGPD.

¹⁶⁸ Art. 6º, inciso IX, da LGPD.

Discrimino também o direito de saída, aspecto de extrema importância no tratamento de dados pessoais. O controlador pode oferecer opções de saídas bem genéricas e a forma como esse *opt-out* se apresenta para o titular será considerado para aumentar ou diminuir a probabilidade do tratamento a partir do legítimo interesse¹⁶⁹. Outra questão passível de questionamentos é a necessidade de justificativas para o titular optar por parar com o tratamento de seus dados.

O §2º do artigo 18 da LGPD prevê que o titular tem o direito de se opor ao tratamento¹⁷⁰ realizado a partir de qualquer base legal que dispensa o consentimento¹⁷¹, desde que haja o descumprimento à Lei. A partir dessa leitura é possível concluir que a justificativa para a paralisação do tratamento pode sim ser requerida pelo titular, contudo, a necessidade de justificativa deverá ser considerada como uma dificuldade na mensuração da proteção de direito de saída no momento do teste de proporcionalidade.

O Considerando 69 da RGPD fala sobre o direito de objeção do titular e mais uma vez fala sobre o ônus do controlador em demonstrar que seu legítimo interesse se sobrepõe à objeção ou interesse do titular. Ou seja, a partir do momento em que o titular se opõe ao tratamento realizado com seus dados a partir da alegação do legítimo interesse do controlador, para continuar tal tratamento o controlador deverá provar que o tratamento é tão necessário naquele caso específico que a vontade do titular não deve prevalecer, evidenciando que no caso concreto os direitos do titular não se sobrepõem aos interesses do controlador¹⁷².

Alguns critérios devem ser sempre considerados na análise de proporcionalidade do tratamento como a natureza do dado. Dados sensíveis¹⁷³ têm um tratamento diferenciado¹⁷⁴ e, por isso, o artigo 11, alínea II, prevê situações específicas que possibilitam o tratamento de

¹⁶⁹ Um instrumento de *opt-out* acessível, com linguagem compreensível e sem maiores justificativas é muito importante para o titular, porque quanto mais compreensível o mecanismo de *opt-out* mais ele se aproxima do *opt-in*, ou seja, do consentimento. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. pp. 43-45;

¹⁷⁰ Sobre o direito de oposição ver Acórdão dos Processos apensos C-141/12 e C-372/12 do TJUE: “Segundo o considerando 25 da Diretiva 95/46/CE, os princípios de proteção das pessoas singulares previstos por esta devem encontrar expressão, por um lado, nas obrigações que impendem sobre as pessoas responsáveis pelo tratamento de dados que dizem respeito àquelas pessoas e, por outro, nos direitos de as pessoas cujos dados são tratados serem informadas sobre esse tratamento, poderem ter acesso aos dados, poderem solicitar a sua retificação e mesmo, em certas circunstâncias, poderem opor-se ao tratamento”.

¹⁷¹ Incisos II a X do artigo 7º da LGPD.

¹⁷² PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. p. 17

¹⁷³ Sobre esse tema, cabe ressaltar que um dado não explicitamente sensível, pode ser demonstrado como sensível. Por exemplo, o sobrenome não é, necessariamente sensível, mas pode demonstrar a origem étnica, o transformando em um dado sensível.

¹⁷⁴ *Ibid.* p. 17.

dados sensíveis¹⁷⁵. Cabe ressaltar que dados sensíveis continuam sendo dados sensíveis mesmo após a sua publicação¹⁷⁶. E, mesmo considerando os dados pessoais fora da categoria de sensíveis, há maior sensibilidade de alguns dados do que outros e isso deve ser considerado no teste¹⁷⁷.

Além disso, deve-se avaliar como será feito o tratamento. Se houver comunicação entre controladores de dados, por exemplo, o tratamento gera maiores consequências e muitas vezes é mais problemático para o titular. Tão importante quanto, são as expectativas do titular e a definição de quem é o controlador e quem é o titular, como já demonstrado ao longo deste trabalho¹⁷⁸.

O objetivo absoluto do teste é evitar impactos desproporcionais, que justifiquem condenações em danos que não responderão às consequências sofridas pelo titular¹⁷⁹. Alguns argumentam que a necessidade desse controle prévio realizado pelo controlador pode enfraquecer o papel da autoridade¹⁸⁰, mas essa conclusão não considera que a autoridade será uma das fontes mais importantes para a criação da forma que o teste deverá ser realizado, definindo padrões e criando seguranças para os agentes envolvidos.

Além disso, deve-se ressaltar que, se o controle anterior ao tratamento for realizado unicamente pelo controlador, algumas questões deverão ser analisadas: a análise proposta requer familiaridade com o tema, então será necessário que alguém especializado participe da confecção do relatório. Ademais, há claro conflito de interesses entre o controlador e a proteção dos dados do titular, porque o controlador obviamente quer possibilitar tal processamento, e, como as sanções são posteriores à prática, é possível que o titular não denuncie o controlador, por inúmeras razões¹⁸¹.

Por isso, o papel da autoridade é de extrema importância, por ser responsável em rever o teste de maneira mais imparcial. Além disso, é necessário incentivar que os titulares tenham papel ativo nas relações que envolvem seus próprios dados, porque essa atuação é essencial para o controle do tratamento, principalmente tendo por base o legítimo interesse. E também é

¹⁷⁵ Vide Seção 3.4. deste trabalho.

¹⁷⁶ No processo C-131/12, o Tribunal de Justiça definiu que: “A conclusão que precede também não é prejudicada pelo facto de esses dados já terem sido publicados na Internet e não serem alterados por esse motor de busca”. Ou seja, a publicação prévia de dados pessoais em nada altera essa classificação.

¹⁷⁷ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. P. 39

¹⁷⁸ Ibid. pp. 39-40

¹⁷⁹ Ibid. p. 41.

¹⁸⁰ PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. p. 22.

¹⁸¹ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. p. 861.

necessário considerar que as empresas deverão criar e/ou melhorar seus programas de *compliance* e controles internos¹⁸²

O resultado final do teste de proporcionalidade feito pelo controlador deverá resultar em um relatório de impacto¹⁸³ que deverá apresentar (i) descrição detalhada do processamento, incluindo a caracterização do legítimo interesse; (ii) demonstração da necessidade e proporcionalidade do tratamento; (iii) demonstração do teste relacionando o legítimo interesse com as consequências para o titular; e (iv) medidas que visam proteger o titular¹⁸⁴.

Abaixo apresento fluxograma com as etapas do teste de proporcionalidade. Esse compilado busca somente apresentar uma forma de se alcançar o relatório de danos que pode ser o produto da prática deste teste, mas os passos aqui retratados não são uma regra, são apenas uma forma segura para o controlador comprovar a prevalência do seu legítimo interesse e, de qualquer forma, o respeito ao princípio da boa-fé, porque ao realizar esse teste de proporcionalidade estará clara a tentativa de seguir a legislação de proteção de dados¹⁸⁵.

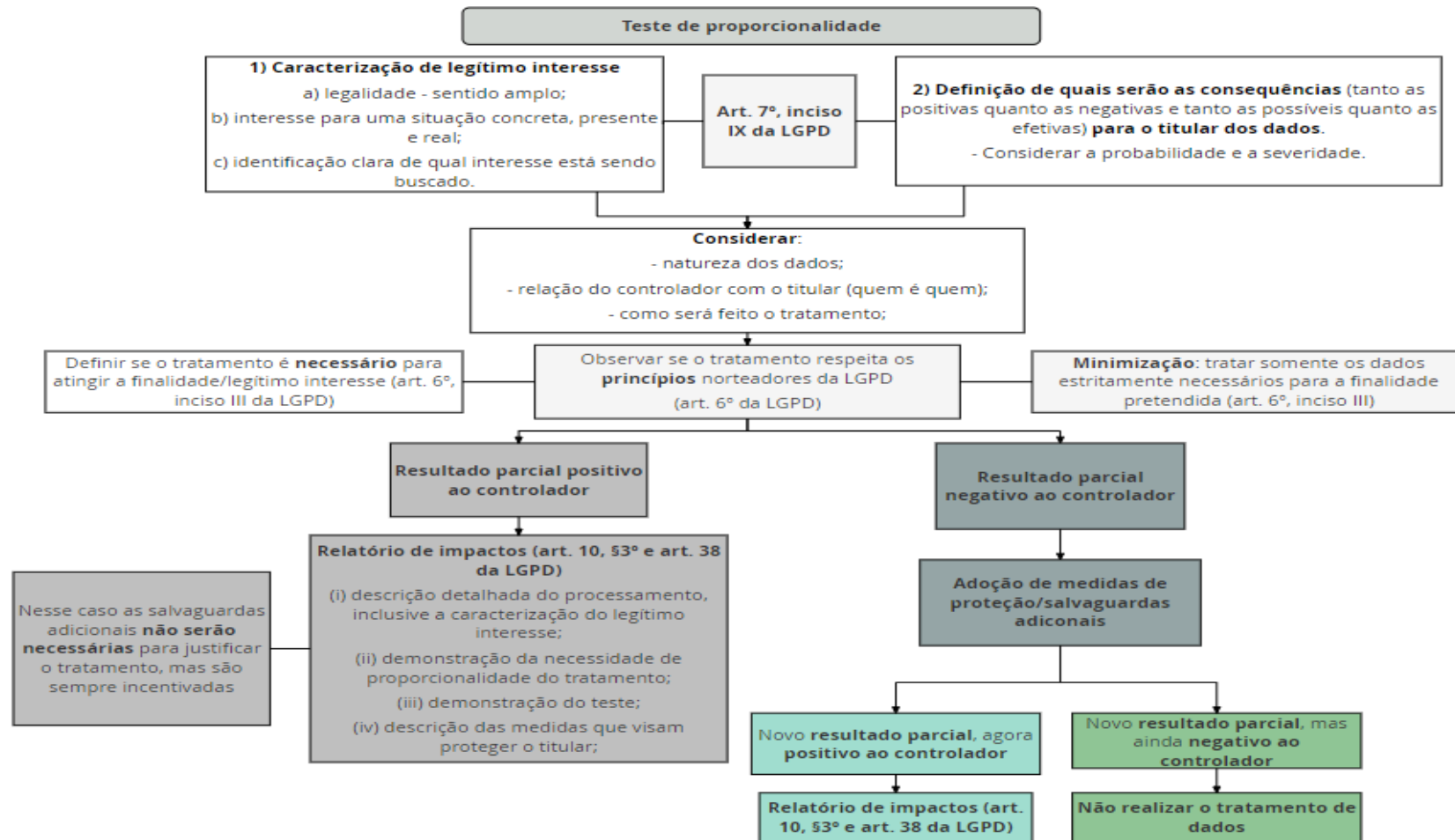
¹⁸² NAUWELAERTS, Wim. *GDPR - The Perfect Privacy Storm: You can Run from the Regulator, but You Cannot Hide from the Consumer*, 3 Eur. Data Port. L. Rev. 2017. pp. 251-256

¹⁸³ Art. 10, §3º da LGPD.

¹⁸⁴ PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. p. 21.

¹⁸⁵ Esse compilado foi feito a partir das leituras feitas para esse trabalho, em destaque ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. e BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019.

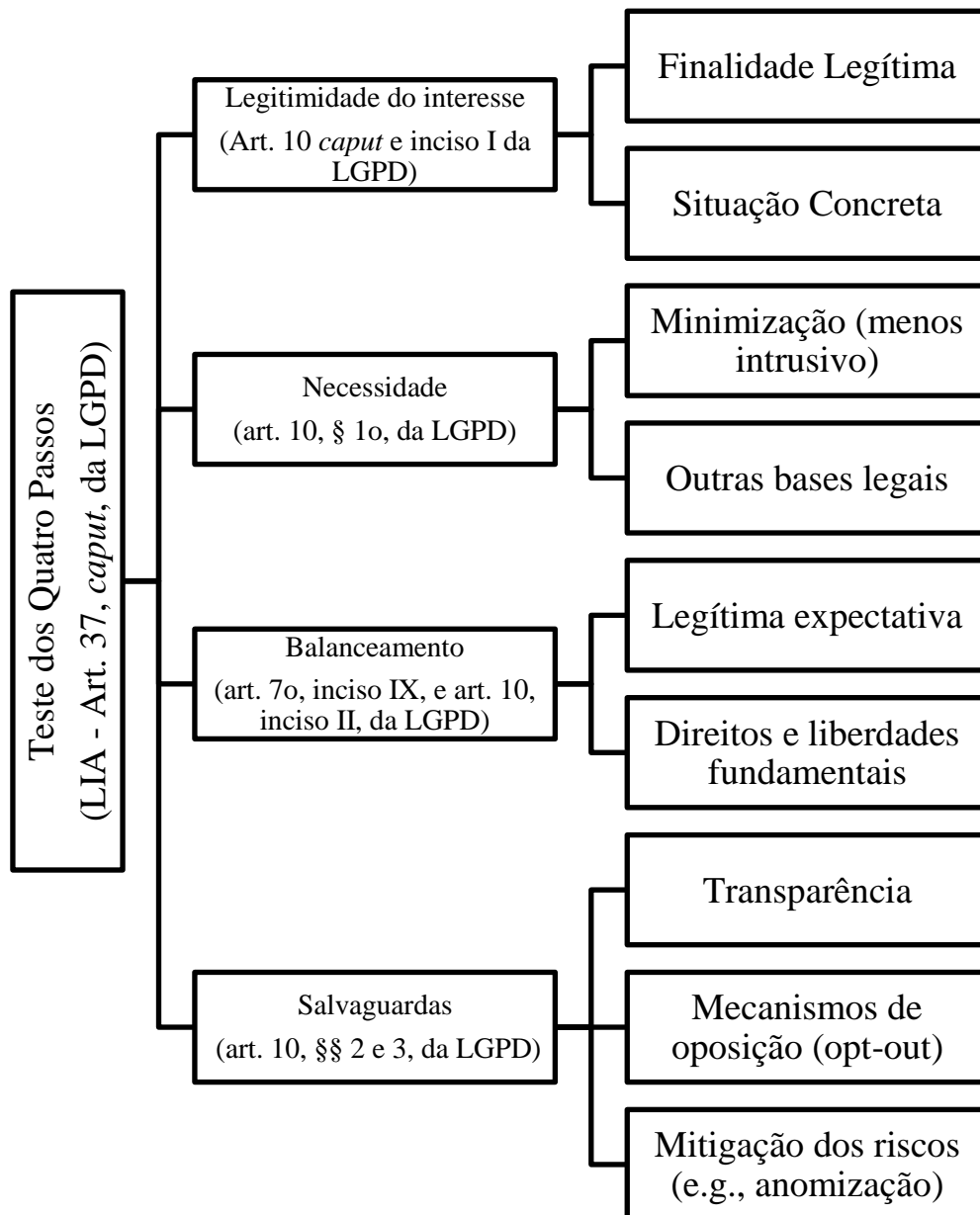
Figura 1 – Fluxograma da Realização do Teste de Proporcionalidade/Confecção do Relatório de Impactos



Fonte: elaborada pela autora

Para fins de comparação, trago a sumarização do teste feita pelo pesquisador Bruno Ricardo Bioni¹⁸⁶, que determina “o teste de proporcionalidade, dividido em quatro estágios, para a aplicação e interpretação do legítimo interesse”:

Figura 2 – Quadro do Teste dos Quatro Passos



Fonte: BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2 Reimpr. Rio de Janeiro: Forense, 2019, p. 256.

¹⁸⁶ BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2 Reimpr. Rio de Janeiro: Forense, 2019, p. 256.

De qualquer forma, o objetivo da realização do teste de proporcionalidade é garantir que haja equilíbrio entre a legítima expectativa do controlador ou do terceiro e os direitos e liberdades fundamentais do titular. Esse equilíbrio pode ser alcançado através de medidas de segurança, as salvaguardas. Para tanto, o teste deve se basear em uma situação concreta e atual e o tratamento de dados deve se demonstrar necessário.

Toda a previsão da necessidade do relatório de impactos perpassa a ideia de que o responsável pelo tratamento de dados deve ser capaz de entender os riscos desse processamento, sendo, assim, a figura mais capaz para antecipar quais medidas previnem esses possíveis danos¹⁸⁷.

3.4. O Legítimo Interesse e os Dados Pessoais Sensíveis

A categoria “dados sensíveis” surgiu a partir da compreensão de que o mau tratamento de tais informações traria danos consideráveis ao titular. A sensibilidade de dados não é algo passível de análise estanque, então são necessárias percepções subjetivas para a caracterização dos dados como sensíveis¹⁸⁸.

O dano inerente à noção de dado sensível é a discriminação. Dessa forma, considera-se que o tratamento diferenciado de dados sensíveis respeito o princípio da isonomia. Afinal, dados que tem como consequência do seu tratamento danos graves devem receber abordagem diferente da dos dados que possibilitam o fluxo informacional - necessário na Era do Big Data -, mas com consequências menores aos titulares¹⁸⁹.

A LGPD definiu, no seu art. 5º, inciso II, dado pessoal sensível como informação que possibilita definir a origem racial ou étnica, posicionamentos religiosos, filosóficos ou políticos, relações sindicais, condições de saúde ou da vida sexual do titular, além de dados biométricos ou genéticos¹⁹⁰. Inclusive como já mencionado no tópico anterior, a LGPD vedou o tratamento de dados sensíveis a partir da base de legitimação “legítimo interesse”.

¹⁸⁷ LIMBERGER, Têmis. *Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu*. Direito digital: direito privado e internet, 2019. P. 256

¹⁸⁸ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. Pp. 31-32.

¹⁸⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. Pp. 85-86.

¹⁹⁰ O art. 5º, inciso II, da LGPD define dados sensíveis: “dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

Essa vedação é entendida a partir da interpretação do artigo 11 da norma geral brasileira. Esse dispositivo cita todas as situações em que o tratamento de dados pessoais sensíveis poderá ocorrer e não menciona o legítimo interesse como base legal para tal processamento. Então, o tratamento desses dados não é terminantemente proibido, mas as bases legais que autorizam o processamento são mais restritivas do que as previstas para o tratamento de dados pessoais - artigo 7 da LGPD.

Por sua vez, a RGPD não define dados sensíveis no artigo 4, item específico sobre definições. Contudo, traz vedação de tratamento a dados que revelam a origem racial ou étnica, opções políticas, religiosas ou filosóficas, filiações sindicais. Além disso, também proíbe o processamento de dados genéticos, biométricos, relacionados à saúde, à vida sexual ou à orientação sexual de indivíduos¹⁹¹. Assim como a norma brasileira, a RGPD traz rol taxativo das situações em que o tratamento de dados pessoais é autorizado e o legítimo interesse do controlador ou de terceiro interessado não é mencionado¹⁹².

Então, tanto a norma brasileira quanto a lei geral europeia sobre proteção de dados pessoais vedaram o processamento de informações pessoais a partir da base legal “legítimo interesse”. Isso pode ser justificado pela assunção feita pelas jurisdições de que o tratamento de dados sensíveis irá gerar danos ao titular¹⁹³. Então, como o tratamento de dados a partir do legítimo interesse deverá considerar as consequências ao titular, como já demonstrado, é possível que a lei proíba tal processamento por considerar que os danos são inerentes ao tratamento. Nesse caso se presume que não há proporcionalidade entre o processamento e os direitos e liberdades do titular.

De qualquer maneira, é necessário ressaltar que apesar da proteção prevista nas legislações, devido a facilidade de associação de dados, a avaliação sobre a sensibilidade dos dados também deverá ser feita caso a caso. Tal fato se dá porque uma informação inicialmente não enquadrável na definição de dado sensível, a partir do cruzamento com outros materiais¹⁹⁴ pode dar ensejo a um perfil que se encaixe nas previsões que caracterizam a sensibilidade¹⁹⁵.

¹⁹¹ Artigo 9, §1º: “*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited*”.

¹⁹² Artigo 9, §2º e alíneas.

¹⁹³ BENNETT, Colin; e RAAB, Charles D. *Revisiting ‘The Governance of Privacy’: Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. Pp. 31-32.

¹⁹⁴ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. Pp. 85-86.

¹⁹⁵ LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo, SP: Editora Saraiva, 2011. Pp. 77-78.

Conclui-se, portanto, que os dados pessoais tidos como não-sensíveis poderão ser tratados a partir da alegação do legítimo interesse do controlador, desde que respeitado o teste de proporcionalidade. A partir de tal teste deve-se buscar verificar se o tratamento de tais dados poderá criar perfil condizente com alguma das hipóteses de classificação da informação como sensível. Nessa hipótese, deve-se adotar medidas que impeçam tal perfilamento, se não o tratamento a partir do legítimo interesse do controlador ou de terceiro resta prejudicado, tendo em vista a vedação ao tratamento de dados pessoais sensíveis a partir do legítimo interesse do controlador.

Contudo, como a sensibilidade dos dados depende também do caso em concreto, o teste de proporcionalidade poderá não vislumbrar que tal perfilamento revela informação sensível. Assim sendo, revela-se novamente a importância da atuação do titular. Com o empoderamento deste sujeito, é provável que este busque formas de impedir o tratamento de dados que permitam a identificação de dados sensíveis de sua privacidade¹⁹⁶.

¹⁹⁶ BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em "Regulation and Governance". Pp. 19 e 31.

CAPÍTULO 4 – O CONCEITO DE LEGÍTIMO INTERESSE A PARTIR DE CASOS CONCRETOS

4.1. Hipóteses de Enquadramento do Legítimo Interesse

O Parecer 06/2014 enumera alguns casos que atualmente são enquadráveis como legítimos interesses da forma prevista no artigo 7, inciso IX, da LGPD: (i) direito à liberdade de expressão ou direito à informação; (ii) marketing direto; (iii) mensagens comerciais não solicitadas; (iv) reivindicações legais; (v) prevenção à fraude no sentido amplo; (vi) monitoramento de empregados; (vii) política de denúncias internas¹⁹⁷; (viii) segurança; (ix) finalidades históricas, estatísticas ou científicas; e (x) pesquisas¹⁹⁸.

Já a doutrina cita outras hipóteses de enquadramento: (a) monitoramento do ambiente de trabalho; (b) operações societárias e processos de troca de informações (*due dilligence*); (c) fraudes e incidentes de segurança; (d) *background-check*: reunião de informações sobre o candidato em processos seletivos; (e) publicidade e marketing (tanto marketing direto quanto marketing indireto e *targeted advertisement*)¹⁹⁹; (f) avaliação de potenciais clientes (*scoring*); (g) melhorias nos serviços ofertados²⁰⁰; entre diversas outras.

Cabe um pequeno desenvolvimento sobre essas hipóteses a fim de comparar o que a doutrina espera na verificação desses casos e o que é efetivamente aplicado pelas Cortes aplicadoras das normativas de proteção de dados pessoais.

O direito à liberdade de expressão²⁰¹ e o direito à informação²⁰² são direitos protegidos constitucionalmente, mas não são absolutos. Por isso, tanto a teoria quanto a prática resguardam limitações a esses direitos como o direito ao esquecimento²⁰³, criminalização de discursos

¹⁹⁷ Em tradução livre, o Departamento para Inovações e Práticas Empresariais, em seu Guia para Empregados e Código de Prática definiu a política de denúncias *whistle-blowing schemes* como: “Denúncia é o termo utilizado quando um funcionário passa informação sobre más condutas (...) A conduta, tipicamente, mas não necessariamente, será algo testemunhado no trabalho”. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415175/bis-15-200-whistleblowing-guidance-for-employers-and-code-of-practice.pdf>.

¹⁹⁸ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p.25

¹⁹⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. pp. 556-568.

²⁰⁰ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. p.862

²⁰¹ Art. 5º, inciso IX, da CF.

²⁰² Art. 5º, inciso XIV, da CF.

²⁰³ Ver “STJ permite que promotora seja esquecida em buscas sobre fraude em concurso”, disponível em: <<https://www.jota.info/coberturas-especiais/liberdade-de-expressao/stj-promotora-esquecida-noticias-fraude-concurso-09052018>>.

contrários aos bens protegidos legalmente tipificando a injúria, calúnia e difamação²⁰⁴. No cenário de proteção de dados pessoais também cabe essa ponderação entre os limites aos direitos e liberdades fundamentais.

As reivindicações legais trazidas pelo Grupo de Trabalho do Artigo 29 como possibilidades para justificar o legítimo interesse dizem respeito ao tratamento de dados para possibilitar persecução eficiente de direitos oriundos principalmente de obrigações provenientes de atos jurídicos, como contratos. Como exemplo, o grupo cita a possibilidade de transferência de dados para um advogado a fim de efetivar pagamento devido, essa transferência poderia ser justificada pelo legítimo interesse, mas é necessário sempre observar se não há compatibilização com outra base legal²⁰⁵.

A prevenção a fraudes (v) é tão essencial à LGPD que mesmo dados sensíveis, que têm seu tratamento autorizado em situações muito específicas, podem ser tratados mesmo sem consentimento do titular como forma de garantir a “prevenção à fraude e a segurança do titular”²⁰⁶.

O combate à fraude interessa não só ao controlador ou a terceiro, porque a sua reputação é de extrema importância para assegurar sua posição no mercado em que a reputação se mostra como fator relevante, mas também para autoridades nacionais e para o próprio titular²⁰⁷. Mas mesmo nesse caso extremo, a cooperação das companhias com autoridades deverá respeitar os princípios de tratamento de dados previstos no artigo 6 da LGPD²⁰⁸.

O combate à fraude tem relação com a configuração baseada em questões de segurança (‘viii’ e ‘c’). É comum que empresas financeiras monitorem as movimentações realizadas pelos clientes a fim de avaliar se alguma atitude é suspeita ao perfil daquele cliente criado pela companhia, o que traz maior segurança inclusive para o cliente²⁰⁹. Mas ainda há questões de segurança ainda mais amplas que podem ser abarcadas pelo legítimo interesse, como por exemplo o uso de câmeras de segurança em lojas para criar provas em casos de práticas de ilícitos²¹⁰.

²⁰⁴ Arts. 138 a 145 do Código Penal Brasileiro.

²⁰⁵ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 60

²⁰⁶ Artigo 11, inciso II, alínea ‘g’ da LGPD.

²⁰⁷ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 35

²⁰⁸ Ibid. p. 22.

²⁰⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. pp. 259-260.

²¹⁰ Observar que essa justificativa para fins de segurança também possibilita a coleta de dados dos funcionários, então também poderá trazer efeitos em outras esferas como a trabalhista.

Ainda na linha de proteção, mas aqui em específico a fim de minimizar os riscos de negócios, é possível vislumbrar algumas das justificativas que podem caracterizar o legítimo interesse como o *scoring* ('f'), monitoramento de empregados ('vi' e 'a'), *background-check* ('d'), e políticas de denúncias internas ('vii').

O primeiro desses se relaciona a segurança do fornecedor de serviços em ter informações satisfatórias sobre o cliente em casos em que a confiança nesse é importante para firmar a relação cliente-fornecedor. É o caso dos provedores de crédito, que avaliam quais condições serão oferecidas com base nas possibilidades desse cliente efetivamente retornar o crédito ao banco²¹¹. Então o processamento dos dados poderia diminuir os riscos do negócio e oferecer condições mais adequadas para os clientes²¹².

Contudo, também é possível tomar atitudes similares para os empregados de uma empresa através do processamento de dados. Por exemplo, a empresa Deliveroo utilizava informações sobre quanto tempo cada entregador demorava para realizar uma entrega, os que demoravam mais recebiam menor pontuação e iam para o final da lista de pontos e quem estava nas últimas colocações tinha maior chance de demissão²¹³.

Dado que os funcionários são essenciais ao funcionamento de uma empresa, as tecnologias que permitem o monitoramento desses durante as jornadas de trabalho e as verificações de informações antes da contratação são instrumentos que facilitam tomadas de decisões empresariais. Contudo, algumas questões devem ser consideradas. Por exemplo, atualmente há dificuldades na divisão do que é privado e do que é relevante para o trabalho. Além disso, tomadas de decisão baseadas em resultados de algoritmos diversas vezes são consideradas incorretas²¹⁴.

Por isso, está claro que as empresas buscarão utilizar tecnologias a fim de incentivar e aumentar o lucro nos negócios²¹⁵, mas deverá informar aos empregados os monitoramentos a que estão sujeitos²¹⁶. O maior problema é que alguns tratamentos são de difícil comprovação,

²¹¹ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. pp. 862-863.

²¹² Sobre esse *scoring* cabe leituras sobre a Lei do Cadastro Positivo, como, por exemplo: BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina. 2018. pp. 152-154. E também MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014. pp. 112-115.

²¹³ CUSTERS, Bart; URSIC, Helena. *Worker Privacy in a Digitalized World Under European Law*. 39 Comp. Lam. L. & Pol'y J. 2018. p. 328.

²¹⁴ Ibid. pp. 323-330

²¹⁵ Idem.

²¹⁶ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. pp. 257-258.

principalmente aqueles feitos antes da contratação²¹⁷. Ademais, o monitoramento não pode ser invasivo, hipótese em que o teste de proporcionalidade entre o legítimo interesse do controlador e os direitos e liberdades do titular acabaria por impedir o tratamento dos dados.

Além disso, a reputação de uma empresa é relevante para aferição de lucros. Na era atual, notícias que impactam a imagem empresarial são rapidamente divulgadas²¹⁸, então há uma tendência entre as empresas de evitar ao máximo esses escândalos. Ademais, as próprias leis brasileiras oferecem vantagens a empresas que possuem políticas de denúncias como *compliances*²¹⁹ ou esquemas *whistleblowing*²²⁰. Contudo, para efetivar tais políticas é necessário que seja feito o tratamento de dados dos funcionários das empresas, por isso a menção a essa hipótese.

Sobre os casos envolvendo *marketing* ('ii', 'iii' e 'e'), deve-se considerar que o Big Data transformou a forma que se dá a publicidade²²¹ e também toda a forma de produção de bens²²². O fornecimento de dados sobre seu comportamento é a sua forma de pagamento para a utilização das eficiências geradas pelo novo modelo de negócios²²³.

Nessa era do Big Data há a clara caracterização da denominada publicidade direcionada²²⁴ que se subdivide em (i) contextual; (ii) segmentada; e (iii) comportamental online²²⁵. A última é de extrema relevância para as companhias e, para que essa ocorra, muitas vezes é necessário que a empresa trate os dados a partir da base legal do legítimo interesse, pela

²¹⁷ CUSTERS, Bart; URSIC, Helena. *Worker Privacy in a Digitalized World Under European Law*. 39 Comp. Lam. L. & Pol'y J. 2018. pp. 323-330.

²¹⁸ Ver, por exemplo, o caso Zara e profissionais em condições análogas à escravidão, disponível em: <<https://www.independent.co.uk/life-style/fashion/zara-labourers-plea-for-help-fast-fashion-business-model-h-m-primark-a8040601.html>>; <<https://www.forbes.com/sites/andersonantunes/2011/08/17/zara-accused-of-alleged-slave-labor-in-brazil/#349a47901a51>>; <<https://economia.estadao.com.br/noticias/geral,zara-pode-entrar-na-lista-suja-de-trabalho-escravo,70002084547>>; <<https://oglobo.globo.com/economia/justica-decide-que-zara-responsavel-por-trabalho-escravo-flagrado-em-2011-22070129>>; <<https://magnet.xataka.com/en-diez-minutos/lo-que-hay-detras-de-la-multa-a-zara-por-trabajo-esclavo-en-brasil-y-el-baile-de-titulares-en-prensa>>.

²¹⁹ Para exemplo, ver Guia para Programas de *Compliance* feito pelo Conselho Administrativo de Defesa Econômica, disponível em: <http://www.cade.gov.br/ acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf>.

²²⁰ A alteração da Lei n. 13.608/2018 apresentada pelo Ministério da Justiça busca a regulamentação do *whistleblowing*, para maiores informações ver: <<https://www.jota.info/opiniao-e-analise/colunas/agenda-anticorrupcao-politicas-publicas/pacote-anticrime-proposta-de-regulamentacao-do-whistleblowing-no-setor-publico-16042019>> e <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/whistleblowing-anteprojeto-moraes-08062018>. Acesso em 30/05/2019.

²²¹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. p. 44.

²²² *Ibid.* p. 48

²²³ *Ibid.*, p. 49. RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Rio de Janeiro: Renovar, 2008. pp. 45-48

²²⁴ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. pp. 15-33.

²²⁵ *Ibid.*, pp. 263-265.

necessidade de coleta de diversos tipos de dados para criação de perfis, e porque o marketing é uma finalidade secundária em diversos casos.

Mais uma vez a situação de hipossuficiência do titular fica clara. As empresas sabem muito sobre os consumidores, porém esses sabem pouco sobre o que é feito com os seus dados, como e para que são utilizados e com quem são compartilhados, etc²²⁶.

Outra categorização de extrema importância é a de marketing direto, indireto ou *targeted advertisement*. O marketing direto é aquele passível de objeção e que deve cessar o tratamento imediatamente²²⁷. Nesse contexto de oferecimento de *opt-out* facilitado, é mais fácil justificar o marketing com base no legítimo interesse, alcançando uma forma do direito de autodeterminação²²⁸, que mesmo sem o consentimento anterior, há ainda um controle sobre os seus dados²²⁹, é uma verdadeira forma de empoderamento do titular para participação e desenvolvimento social²³⁰. Como mencionado anteriormente, a existência de relação anterior entre o titular e o controlador faz com que o tratamento posterior dos dados seja esperado pelo titular²³¹. A partir dessa interpretação, é possível a compreensão de que o marketing direcionado a um cliente antigo é caso de publicidade direta. Já o marketing indireto é aquele utilizado para angariar novos clientes.

A Diretiva de ePrivacy da União Europeia prevê a necessidade de consentimento para alguns casos específicos de marketing²³². Isso se deu pelo entendimento de que estruturas de marketing cada vez rastrearam mais atividades para gerar perfis de consumo, o que justificou o entendimento de que muitas vezes o *opt-out* não supre os direitos do titular²³³. Tal fato mostra a possível fragilidade do marketing na caracterização de legítimo interesse.

²²⁶ Ibid. p. 28.

²²⁷ Ibid. p. 264 e ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 14.

²²⁸ A autodeterminação é mais ampla do que o consentimento. Agrega também o domínio dos dados. Dessa forma, se os dados forem tratados de forma totalmente previsível, em consonância com as legítimas expectativas do titular, pode gerar o “consentimento contextual”. BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019. p. 268-273.

²²⁹ SCHWABE, Jürgen. *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Uruguay: Konrad-Adenauer-Stiftung E.V. 2005. pp. 236-238.

²³⁰ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. pp. 850-81

²³¹ Considerando 47 da RGD,.

²³² ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 46: “the requirement for consent under Article 13 of the ePrivacy Directive for automated calling systems, fax, text messages and e-mail marketing (subject to exceptions), and de facto application of Article 7(a) of the Data Protection Directive; the requirement for consent under Article 5(3) of the ePrivacy Directive (and Article 7(a) of the Data Protection Directive) for behavioural advertising based on tracking techniques such as cookies storing information in the terminal of the user”.

²³³ Ibid. p. 46.

A RGPD traz previsões específicas sobre o *marketing* direto em seu artigo 21²³⁴. Já a lei nacional não faz menção específica a esse instituto, aplicando-se a ele as regras gerais. Ressalta-se que, muitas vezes, a publicidade é uma finalidade secundária do controlador, o que pende a balança para as questões do titular²³⁵.

A alegação de melhoria do serviço ofertado (g) pode ser vista como forma de efetivamente aprimorar plataforma já existente, como o Google, que processa dados para melhorar a experiência do consumidor²³⁶. Mas também há casos em que o tratamento de dados é essencial para o próprio funcionamento da plataforma, como por exemplo o aplicativo “Lulu” que utilizava de dados de redes sociais para criar perfis de homens que seriam avaliados anonimamente por garotas. Se não possuísse o acesso a tais dados, o Lulu não conseguiria funcionar²³⁷.

O questionamento sobre a utilização dessa justificativa na caracterização do legítimo interesse fica claro quando pensamos nas consequências negativas que podem advir de uma má avaliação feita neste último aplicativo. Esse foi o motivo para um dos titulares dos dados utilizados na construção do Lulu ter judicializado tal processamento, pedindo danos morais à rede social, porque ele se sentiu prejudicado, ofendido pelas avaliações²³⁸.

Por fim, o tratamento de dados para fins científicos (‘ix’ e ‘x’) é feito em basicamente todas as produções acadêmicas, como no presente trabalho, e para criação de políticas públicas²³⁹. Contudo, os trabalhos técnicos sempre encontraram limitações éticas²⁴⁰, devido aos possíveis desdobramentos do processamento dos dados, o que também deverá ser observado com nas consequências dos titulares dos dados.

²³⁴ Artigo 21, 2 “Where personal are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing”. Artigo 21, 3: “Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes”.

²³⁵ ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. p. 47.

²³⁶ FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. p.864

²³⁷ BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina. 2018. pp.129-132.

²³⁸ Ibid, pp.129-130.

²³⁹ “Lei do censo”, discutida no trabalho: SCHWABE, Jürgen. *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Organização e Introdução de Leonardo Martins. Tradução de Beatriz Henning, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Geraldine Ferreira. Uruguay: Konrad-Adenauer-Stiftung E.V. 2005.

²⁴⁰ Para maior aprofundamento, ver, por exemplo, RUSSO, Marisa. *Ética e integridade na ciência: da responsabilidade do cientista à responsabilidade coletiva*, 2014. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142014000100016>.

Contudo, as listas de hipóteses de caracterização do legítimo interesse são meramente exemplificativas, justificando o pleito da necessidade das avaliações caso-a-caso, de acordo com os tópicos anteriores. Então, é possível que, com a prática e a aplicação das legislações, apareçam novas hipóteses ainda não previstas pelos pesquisadores da área. Por isso, o objetivo almejado a seguir é identificar se essas hipóteses já foram caracterizadas na prática. Para tanto, foi feito um estudo qualitativo de casos já julgados pelo Tribunal de Justiça da União Europeia.

4.2. Casos Concretos

Para compreender melhor como o legítimo interesse está sendo caracterizado em casos concretos, foi feita uma pesquisa jurisprudencial no site do Tribunal de Justiça da União Europeia²⁴¹, através da modalidade “pesquisa avançada”. Como recorte temporal foi utilizada a opção “desde há 5 anos”, opção já fornecida pela própria ferramenta de buscas.

A escolha em avaliar a jurisprudência do TJUE é justificada pela semelhança entre a Diretiva 95/46/CE e a RGPD e a lei geral brasileira - LGPD. Também há de se considerar que a jurisdição europeia é a principal influência global sobre o tema²⁴². Além disso, Cortes Internacionais são fundamentais para a política de proteção de dados²⁴³, principalmente no que tange a interpretação de conceitos incertos das leis gerais e ao se considerar a tendência global de proteção de dados²⁴⁴.

Sobre os filtros utilizados para a pesquisa buscou-se somente casos de matéria de “proteção dos dados” e foram utilizados alguns filtros na caixa “palavras do texto”, seriam eles: (i) “interesse legítimo”; (ii) “legítimo interesse”; (iii) “interesses legítimos”; (iv) artigo 6(f)²⁴⁵; (v) artigo 6 alínea f; (vi) artigo 7 alínea f²⁴⁶. A seguir, segue cópia da página de buscas do site para compreensão de como foi feita a pesquisa:

²⁴¹ A consulta eletrônica da jurisprudência do TJUE pode ser feita através do link: <<http://curia.europa.eu/juris/recherche.jsf?language=pt>>. Acesso em março e abril de 2019.

²⁴² BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em “*Regulation and Governance*”. P. 8.

²⁴³ Sobre o tema, ver (Ibid), p. 8: “*The role of international courts did not feature in GoP [The Governance of Privacy: Policy Instruments in Global Perspective] (nor did the effect of national case-law). They are now absolutely central to national and international data protection policy, and the future interpretation of many of the GDPR's unclear provisions.*”

²⁴⁴ Ibid. P. 8.

²⁴⁵ Artigo que prevê o legítimo interesse na RGPD;

²⁴⁶ Artigo que prevê o legítimo interesse na Diretiva 95/46/CE.

Figura 3 – Página de Pesquisa Jurisprudencial do TJUE

Estado dos processos	? <input checked="" type="radio"/> Todos os processos <input type="radio"/> Processos encerrados <input type="radio"/> Processos pendentes
Jurisdição	? <input checked="" type="checkbox"/> Todas <input checked="" type="checkbox"/> Tribunal de Justiça <input checked="" type="checkbox"/> Tribunal Geral <input checked="" type="checkbox"/> Tribunal da Função Pública
Número de processo	? <input type="text"/> (ex: C-17/05; 17/05)
Nome das partes	? <input type="text"/>
Documentos	? <input type="text" value="Todos"/>
ECLI	? <input type="text" value="ECLI:EU:"/>
Palavras do texto	? <input type="text" value="VARIÁVEL"/>
Período ou data	? <input type="text" value="Data da prolação"/> <input type="radio"/> de <input type="text" value="11/04/2014"/> a <input type="text" value="11/04/2019"/> (dd/mm/aaaa) <input type="radio"/> desde há 8 dias <input type="radio"/> desde há 1 mês <input type="radio"/> desde há 1 ano <input checked="" type="radio"/> desde há 5 anos <input type="radio"/> em <input type="text"/> (dd/mm/aaaa)
Matéria	? <input type="text" value="Proteção dos dados"/>
Processo e resultado	? <input type="text"/>
Citações de jurisprudência ou de legislação	? pesquisar em <input checked="" type="checkbox"/> Fundamentos <input type="checkbox"/> Dispositivo <input type="checkbox"/> Pedidos Categoria <input type="text"/>
Plano de classificação sistemática	? <input type="text"/> <input checked="" type="checkbox"/> Alargar ao antigo/novo plano
Formação de julgamento	? <input type="text"/>
Juiz-relator	? <input type="text"/>
Advogado-geral	? <input type="text"/>
Origem de uma questão prejudicial	? <input type="text"/>
Língua que faz fé	? <input type="checkbox"/> Língua do processo <input type="checkbox"/> Língua das conclusões <input type="text"/>
Observações e sugestões	

Fonte: elaboração da autora a partir do sítio eletrónico

<<http://curia.europa.eu/juris/recherche.jsf?redirection=doc&oqp=&for=&mat=or&lgrec=pt&jge=&ordreTri=dateDesc&td=%24mode%3D8D%24from%3D2019.06.04%24to%3D2019.06.11%3B%3B%3BPUB1%2CPUB3%2CPUB4%3BNPUB1%3B%3BORDALL&jur=C&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=8733265>>. Acesso em 11/06/2019.

Ainda, foi feita a busca jurisprudencial no site em inglês das publicações do Tribunal com o seguinte critério de busca: “*Domain: EU law and case law. Subdomain: case law. Subject matter: Data Protection. Date: All dates, from 01/04/2014 to 01/04/2019. Results containing ‘legitimate interest’ in title and text. Search language: English*”. Nenhum dos resultados dessa busca foi inédito em relação à busca anterior.

Dessa forma, a pesquisa alcançou o seguinte compilado de casos. Foram analisados os acórdãos disponibilizados em português ou em francês, então, foram excluídos do estudo os processos Avis 1/15, C-40/17, C-708/18, F-57/14, T-652/16 P e T-684/15 P:

Tabela 2 – Resultados da Busca Quantitativa da Jurisprudência do TJUE

Número do processo	Busca “interesse legítimo”	Busca “legítimo interesse”	Busca “interesses legítimos”	Busca “artigo 6(f)”	Busca “artigo 7 alínea f”	Busca “artigo 6 alínea f”	Busca “legitimate interest”	Acórdão disponível
Avis 1/15	Sim	Não	Não	Sim	Não	Sim	Não	Não, somente conclusões
C-13/16	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
C-25/17	Não	Não	Não	Sim	Não	Sim	Não	Sim
C-127/13	Não	Não	Não	Sim	Não	Sim	Não	Sim
C-131/12	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
C-141/12	Não	Sim	Sim	Sim	Não	Sim	Sim	Sim
C-191/15	Sim	Não	Não	Sim	Não	Sim	Sim	Sim
C-201/14	Não	Não	Sim	Sim	Não	Sim	Não	Sim
C-203/15	Não	Não	Sim	Sim	Não	Sim	Não	Sim
C-210/16	Não	Não	Não	Sim	Não	Sim	Não	Sim
C-212/13	Não	Não	Sim	Sim	Sim	Sim	Não	Sim
C-230/14	Não	Não	Não	Sim	Não	Sim	Não	Sim
C-235/14	Não	Não	Sim	Sim	Não	Sim	Não	Sim
C-345/17	Não	Não	Sim	Sim	Sim	Sim	Não	Sim
C-362/14	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
C-398/15	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim

Número do processo	Busca “interesse legítimo”	Busca “legítimo interesse”	Busca “interesses legítimos”	Busca “artigo 6(f)”	Busca “artigo 7 alínea f”	Busca “artigo 6 alínea f”	Busca “legitimate interest”	Acórdão disponível
C-40/17	Sim	Não	Sim	Não	Sim	Não	Não	Não
C-424/15	Não	Não	Não	Sim	Não	Sim	Não	Sim
C-434/16	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
C-446/12	Não	Não	Sim	Sim	Não	Sim	Não	Sim
C-536/15	Não	Não	Não	Sim	Não	Sim	Não	Sim
C-582/14	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
C-615/13	Sim	Não	Sim	Não	Não	Não	Sim	Sim
C-708/18	Sim	Não	Sim	Não	Sim	Não	Não	Não
C-73/16	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
F-57/14	Não	Não	Sim	Sim	Não	Sim	Não	Somente em francês
T-115/13	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
T-343/13	Não	Não	Não	Sim	Sim	Sim	Sim	Sim
T483/13	Não	Não	Não	Sim	Não	Sim	Não	Sim *em inglês
T-493/13	Não	Não	Não	Sim	Não	Sim	Não	Sim
T-652/16 P	Não	Não	Não	Sim	Não	Não	Não	Somente em francês
T-684/15 P	Não	Não	Não	Sim	Não	Não	Não	Somente em francês

4.3. Avaliação dos Casos Concretos

4.3.1. Direito à Liberdade de Expressão ou Direito à informação

No caso *Google Spain vs. Mario Costeja González*²⁴⁷, o legítimo interesse foi a justificativa utilizada pelo Google para o tratamento dos dados do Sr. González e ele foi definido através do interesse econômico do operador em processar tais dados e também porque há interesse de terceiros, o público em geral, em ter acesso a tais informações.

Esses interesses foram superiores ao interesse do titular, contudo, com o passar do tempo, as consequências para o titular ficaram desproporcionais aos interesses de terceiros e do controlador dos dados, então a caracterização de “legitimidade” foi perdida com o tempo. Essa conclusão foi possível inclusive pela finalidade do Google, ou seja, o acesso a informações atuais e relevantes, e, por isso a indexação não é feita para fins históricos, científicos ou estatísticos, como depreendido dos seguintes trechos da decisão:

“Com a sua terceira questão, o órgão jurisdicional de reenvio pergunta, em substância, se os artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que permitem à pessoa em causa exigir ao operador de um motor de busca que suprima da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome dessa pessoa, as ligações a páginas *web* publicadas legalmente por terceiros e que contenham informações verdadeiras sobre ela, com o fundamento de que essas informações são suscetíveis de a prejudicar ou de que deseja que sejam «esquecidas» decorrido algum tempo.

(...)

Quanto ao artigo 12.º, alínea b), da Diretiva 95/46, cuja aplicação está subordinada à condição de que o tratamento de dados pessoais seja incompatível com esta diretiva, importa recordar que, como salientado no n.º 72 do presente acórdão, essa incompatibilidade pode resultar não só do facto de esses dados serem inexatos mas, em especial, também do facto de serem inadequados, não pertinentes ou excessivos atendendo às finalidades do tratamento, de não estarem atualizados ou de terem sido conservados durante um período de tempo superior ao necessário, a menos que a sua conservação se imponha para finalidades históricas, estatísticas ou científicas. Decorre destas exigências, previstas no artigo 6.º, n.º 1, alíneas c) a e), da Diretiva 95/46, que mesmo um tratamento inicialmente lícito de dados exatos se pode tornar, com o tempo, incompatível com esta diretiva, quando esses dados já não sejam necessários atendendo às finalidades para que foram recolhidos ou tratados. Tal é o caso, designadamente, quando são objetivamente inadequados, quando não são pertinentes ou já não são pertinentes ou quando são excessivos atendendo a essas finalidades ou ao tempo decorrido”

O caso *Google Spain* demonstra que o resultado do teste de proporcionalidade é mutável com o decorrer de tempo, ou seja, há um quesito temporal que deve ser considerado na

²⁴⁷ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Seção), caso C-131/12, 13 de maio de 2014. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

caracterização do legítimo interesse além do interesse econômico e do acesso à informação, motivos que podem justificar o tratamento de dados por caracterizarem um interesse legítimo.

As conclusões do Tribunal de Justiça da União Europeia no caso C-345/17²⁴⁸ demonstram que a liberdade de expressão muitas vezes tem relação com um trabalho jornalístico, mas, essa finalidade, produção de notícias, é abrangido por outras isenções. Por isso, o tratamento não deve ser feito a partir da mera alegação do legítimo interesse existente no direito ao acesso à informação, mas sim a partir das regulações referentes à finalidade jornalística.

A legislação brasileira traz a ressalva de que a LGPD não se aplica ao tratamento de dados pessoais realizado para fins jornalísticos²⁴⁹, então, o acesso à informação pode caracterizar um legítimo interesse para o tratamento dos dados, mas não quando se tratar de processamento para essa finalidade apenas, hipótese em deverão ser aplicadas as regras específicas.

4.3.2. Finalidades Históricas, Estatísticas ou Científicas

O caso Google Spain citado no tópico anterior basicamente caracterizou o legítimo interesse a partir do direito ao acesso à informação. Contudo, ressaltou que finalidades históricas, estatísticas ou científicas também podem justificar o tratamento de dados, mas para tanto, esses dados se diferem daqueles oferecidos na busca do nome do Sr. González na plataforma Google.

4.3.3. Segurança Pública

Ainda sobre questões de segurança, evitando a prática de crimes ou possibilitando a produção de provas para condenação de um ilícito, pode-se citar o Acórdão do processo C-212/13²⁵⁰, autos em que foi discutida a possibilidade de um particular tratar imagens de câmera de segurança no seu imóvel, que filma inclusive ruas públicas, a fim de reconhecer quem causou danos ao bem.

²⁴⁸ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-345/17, 14 de fevereiro de 2019. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=210766&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁴⁹ Art. 4, inciso II, alínea 'a' da LGPD.

²⁵⁰ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Quarta Seção), caso C-212/13, 11 de dezembro de 2014. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

O TJUE afirmou que esse sistema de gravação não é uma atividade exclusivamente pessoal ou doméstica, mas o tratamento dos dados nesse caso, a fim de reconhecimento do autor do ilícito, pode caracterizar o legítimo interesse para o processamento de dados.

O acórdão do processo C-582/14²⁵¹ afirmou que não pretende definir o que é “legítimo interesse”, mas determina que nenhuma lei nacional de algum Estado-Membro pode restringir essa categoria, que deverá ser definida caso a caso. Nessa situação específica, as características demonstram que o legítimo interesse poderia existir para garantir a segurança pública.

Um entendimento semelhante poderia ser aplicado no Brasil ao passo que nenhuma lei esparsa deverá restringir o âmbito de aplicação da categoria “legítimo interesse”. Também fica claro que a segurança é finalidade que se encaixa como um interesse legítimo, principalmente nas situações em que os efeitos ao titular são minimizados.

4.3.4. Segurança da Informação

O julgamento do processo C-434/16²⁵² versava sobre um cidadão tentando acessar suas folhas de resposta de provas para exercer categoria profissional. O acórdão definiu que a negativa de que informações referentes a um candidato em exame profissional são dados pessoais afasta a legitimidade do tratamento desses dados. Ou seja, a partir da afirmação que tais dados são pessoais, o seu tratamento seria legítimo. Mas o Tribunal reforçou que o acesso a tais dados deve ser garantido, bem como o direito à retificação e aos pedidos de destruição. As possíveis alterações não devem ser sobre o conteúdo das respostas do titular, essas informações devem ser preservadas na forma original de modo que o tratamento seja justo a todos os candidatos.

4.3.5. Riscos do Negócio

²⁵¹ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-582/14, 19 de outubro de 2016. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁵² TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-434/16, 20 de dezembro de 2017. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

O processo C-201/14²⁵³ conclui que há um legítimo interesse do controlador em tratar dados pessoais para qualificar sujeitos e também para possibilitar cobrança de contribuições em atraso, ou seja, é possível o tratamento para minimizar pagamentos não realizados.

Apesar deste caso versar sobre um interesse legítimo de um Estado, raciocínio semelhante pode ser aplicável a empresas que podem criar perfis de clientes para disponibilizar créditos, por exemplo. Tais ações como o *scoring* minimizam riscos de negócios e, por isso, tal processamento é feito inclusive por órgãos estatais, como no caso do mau pagador que tem seu nome disponibilizado no SERASA, até mesmo esse compartilhamento de dados do órgão estatal com empresas interessadas caracteriza tratamento de dados pessoais, mas pode ser justificado pelo legítimo interesse das empresas em ter tais informações. Ademais, as consequências podem ser mitigadas por medidas adotadas pelo controlador, como maior transparência, facilidade na retificação de dados incorretos e proteção contra discriminação.

Outro processo que demonstra a importância do tratamento de dados para amenizar riscos inerentes ao negócio é o C-398/15, em que o Sr. Salvatore Manni pedia a desassociação dos seus dados com os da falência de sua antiga empresa, porque tais informações foram processadas “por uma sociedade especializada na recolha [sic] (recolhimento) e processamento de informação de mercado e na evolução dos riscos (*rating*)”²⁵⁴.

O acórdão definiu que há interesse legítimo no tratamento desses dados para ter maior segurança jurídica nas relações comerciais. A alegada “não venda” do imóvel de titularidade do Sr. Salvatore devido a publicidade dos dados relativos à falência não justificam *per se* o fim do tratamento desses dados, porque a impossibilidade de venda pode ser oriunda de diversos outros motivos, então, o interesse sobre o tratamento é muito maior do que o do titular.

4.3.6. Reivindicações Legais

No âmbito do Processo C-13/16²⁵⁵, a empresa “Rigas” solicitou acesso ao nome, endereço, número de identidade e cópia de declarações à “Polícia Nacional” da Letónia de uma

²⁵³ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Terceira Seção), caso C-201/14, 01 de outubro de 2015. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=168943&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁵⁴ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-398/15, 09 de março de 2017. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁵⁵ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-13/16, 04 de maio de 2017. Disponível em:

peessoa que causou danos à empresa, a fim de entrar com processo de indenização contra esse agente. Contudo, a Polícia só forneceu o nome completo do agente, porque esse era menor e a legislação nacional prevê as pessoas às quais a Polícia pode compartilhar tais informações.

No caso concreto, a decisão do Tribunal de Justiça da União Europeia definiu que não há obrigação do controlador dos dados em compartilhar dados pessoais com terceiro para que esse possa atingir seus interesses legítimos, mas também não há nenhum impedimento sobre essa ação. De qualquer forma, a decisão salientou que o interesse legítimo do terceiro interessado estava claro, porque esse objetivava tratar essas informações para possibilitar a persecução de possível indenização.

4.3.7. Marketing

O processo C-210/16²⁵⁶ não versa explicitamente sobre o legítimo interesse do controlador, pois o maior foco das questões levantadas nos autos diz respeito à determinação de quais agentes seriam considerados responsáveis pelo tratamento de dados pessoais. De qualquer forma, o acórdão aproveitou a oportunidade para versar sobre a finalidade do tratamento dos dados coletados pelo Facebook a partir de visitas de usuários aos “serviços Facebook, os propostos por outras companhias Facebook e por outras empresas que utilizam os serviços Facebook”, afirmando que o tratamento desses dados pessoais possibilita aprimoramento do sistema publicitário da empresa.

Ou seja, como a legitimidade do tratamento não foi questionada, conclui-se que a melhora no marketing oferecido pela empresa é justificativa razoável para o tratamento de dados pessoais dos usuários da plataforma.

O caso C-230/14 também versa sobre um caso que o tratamento de dados pessoais era utilizado para finalidades publicitárias. Contudo, se tratava do processamento de informações dos próprios anunciantes para a divulgação de imóveis. Ou seja, é possível que o tratamento tenha sido realizado com base no consentimento do titular ou de forma a concretizar previsões contratuais. Como o caso não se deteve a detalhes sobre isso, porque a questão principal era sobre a aplicação territorial da Diretiva 95/46/CE, o caso se mostra relevante para a análise desse trabalho ao passo que demonstra que a finalidade publicitária pode ser buscada através

<<http://curia.europa.eu/juris/document/document.jsf?text=&docid=190322&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1309585>>. Acesso em abril de 2019.

²⁵⁶ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Seção), caso C-210/16, 05 de junho de 2018. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1352637>>. Acesso em abril de 2019.

de outras bases legais para o tratamento, evidenciando que o legítimo interesse só deve ser alegado quando houver efetivamente a sua caracterização e não de outra justificativa para o tratamento.

4.3.8. Demais Hipóteses

Nenhum caso analisado fez menção direta às demais hipóteses citadas como possibilidades para caracterização do legítimo interesse. Ou seja, o trabalho não viu a configuração do legítimo interesse através do envio de mensagens comerciais não desejadas, como forma de garantir a prática de políticas de denúncias internas, nem para monitoramento de empregados (nem antes da contratação nem posterior), tampouco para evitar fraudes ou para viabilizar pesquisas.

Isso pode ser justificado pelas situações ou porque se enquadrarem em outras bases legais ou até mesmo por falta de contestação por parte dos titulares, que também pode se dar por inúmeras razões. O fato é, o Tribunal de Justiça da União Europeia ainda não julgou nenhum caso que enquadre essas previsões em legítimo interesse para o tratamento dos dados, mas deixou claro em diversos acórdãos que o “legítimo interesse” pode ser caracterizado a partir das mais diversas justificativas, inclusive possibilidades ainda não pensadas e que nenhum rol deverá ser taxativo para essas hipóteses.

Além disso, houve uma limitação temporal dos casos estudados, então, decisões anteriores da Corte não foram avaliadas, mas poderiam versar sobre as demais hipóteses, fornecendo guias para as práticas futuras.

4.3.9. Outros Casos Concretos

Nem todos os casos que apareceram no resultado da pesquisa versavam sobre o tratamento de dados pessoais baseado no legítimo interesse. Aqui, busca-se demonstrar quais os conteúdos dos demais processos que apareceram como resultado da busca.

O processo C-191/15²⁵⁷ definiu que durante a vigência da Diretiva 95/46/CE, o direito nacional aplicável é aquele onde efetivamente ocorre o tratamento dos dados pessoais, quando houver compartilhamento de dados entre Estados-membros.

²⁵⁷ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Terceira Seção), caso C-191/15, 28 de julho de 2016. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=182286&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

Os processos apensos C-203/15 e C-698/15²⁵⁸ também versaram sobre compatibilidade de legislações em relação a “conservação generalizada e indiferenciada dos dados relativos às comunicações eletrônicas”, concluindo que as previsões da Carta dos Direitos Fundamentais da União Europeia se opõe à chamada “conservação generalizada e indiferenciada” dos dados de assinantes, mas ressalvando que em casos de luta contra a criminalidade, tal entendimento pode sim ser flexibilizado, mas sempre deverá existir medidas para afastar as chances de abusos.

Já o acórdão referente aos processos apensos C-446/12 a C-449/12²⁵⁹, responde questões referentes à interpretação do Regulamento (CE) n° 2252/2004²⁶⁰, que cuida de documentos de identidade de duração de até 12 meses e passaportes temporários. O julgamento determinou que um Estado-membro pode criar leis de dados biométricos utilizados para confecção de tais documentos, indo além dos fins estabelecidos no próprio regulamento, que prevê que os dados podem ser utilizados até para verificar a autenticidade dos documentos confeccionados pelo Estado. Ou seja, mesmo os dados biométricos podem ser tratados para atender finalidades não iniciais, podendo ser caracterizado inclusive o legítimo interesse. Contudo, o acórdão não trata da caracterização dessa categoria.

O caso C-362/14²⁶¹ versa sobre o compartilhamento de dados do Facebook Irlanda com o Facebook Estados Unidos da América. O julgamento determinou estar claro que o tratamento de tais dados é necessário para atingir o “interesse público” de efetivo funcionamento da plataforma. Mas o Tribunal aproveitou a oportunidade para confirmar que o direito de oposição do titular pode ser utilizado para a realização de pedidos de investigação e que esse pedido do titular já seria razão suficiente para gerar o exame pormenorizado do tratamento dos dados. A oposição do titular surgiu por acreditar que seus dados não estariam suficientemente protegidos devido à legislação mais branda existente nos EUA sobre o tema de proteção de dados pessoais.

²⁵⁸ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Seção), casos: C-203/15 e C-698/15 (apensos), 21 de dezembro de 2016. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁵⁹ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Quarta Seção), casos: C-446/12, C-447/12, C-448/12 e C-449/12 (apensos), 16 de abril de 2015. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=163716&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁶⁰ Regulamento (CE) n° 2252/2004 do Conselho, de 13 de dezembro de 2004, que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros.

²⁶¹ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Seção), caso C-362/14, 06 de outubro de 2015. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

Sobre esse caso, há uma correlação com o julgamento do caso já citado C-210/16, porque neste o TJUE determinou que um Estado-Membro poderia exercer todos os poderes conferidos pela Diretiva 95/46/CE em relação ao tratamento de dados realizado pelo grupo Facebook, mesmo que territorialmente o Estado-Membro tivesse instalado na região apenas um ponto responsável por vendas publicitárias. Isso nas situações em que a empresa dispusesse de estabelecimentos em diversos Estados-Membros. Essa intervenção no tratamento dos dados feito pelo grupo empresarial detentor dos diversos estabelecimentos independe de solicitação de intervenção da autoridade do Estado em que se fixa a sede da empresa.

O TJUE definiu, no julgamento do processo C-25/17²⁶², que a liberdade religiosa inclui a pregação, mas, como no caso, as Testemunhas de Jeová estavam colhendo dados sobre quem visitavam e os processando, o Tribunal confirmou que essa atividade não caracteriza atividade exclusivamente de pessoas ou doméstica. Os dados coletados pelas Testemunhas recebiam tratamento manual e estavam submetidos à aplicação da Diretiva 95/46/CE, porque os dados pessoais eram estruturados, caracterizando assim tratamento não-automatizado de dados pessoais. O acórdão definiu, por fim que a Comunidade de Testemunhas de Jeová é conjuntamente responsável com os membros pregadores pelo tratamento dos dados coletados, visto que incentiva e coordena tais ações, independentemente de ter efetivo acesso a elas.

O processo C-615/13 P, tramitado no Tribunal de Justiça da União Europeia, tinha como objeto o requerimento de acesso aos dados completos, incluídos os nomes dos peritos responsáveis pela elaboração de pareceres que orientaram a Autoridade Europeia para a Segurança dos Alimentos (EFSA). O Tribunal de Justiça deu provimento²⁶³ ao recurso

²⁶² TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Seção), caso C-25/17, 10 de julho de 2018. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁶³ Trata-se de recurso de uma decisão do Tribunal Geral, interposto ao abrigo do artigo 56 do Estatuto do Tribunal de Justiça da União Europeia. De acordo com o Estatuto do Tribunal de Justiça da União Europeia, quando este Tribunal anula a decisão do Tribunal Geral, pode decidir definitivamente o litígio, como foi feito no mencionado caso. Vide TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-615/13 P, 16 de julho de 2015, itens 62, 63, 73 e 75: “De acordo com o artigo 61.º, primeiro parágrafo, segundo período, do Estatuto do Tribunal de Justiça da União Europeia, quando este Tribunal anula a decisão do Tribunal Geral, pode decidir definitivamente o litígio, se estiver em condições de ser julgado. No caso, o Tribunal de Justiça considera que o recurso de anulação da decisão da EFSA de 12 de dezembro de 2011, interposto pela ClientEarth e pela PAN Europe, está em condições de ser julgado, devendo, por conseguinte, ser definitivamente decidido. (...) Consequentemente, há que dar provimento ao recurso de primeira instância e anular a decisão da EFSA de 12 de dezembro de 2011. (...) Tendo sido dado provimento ao recurso de segunda instância da ClientEarth e da PAN Europe e ao recurso de primeira instância interposto no Tribunal Geral, a EFSA suportará as suas próprias despesas e deve ser condenada nas despesas da ClientEarth e da PAN Europe no processo de recurso em segunda instância e no processo de primeira instância, de acordo com o pedido destas últimas. A Comissão suportará as suas próprias despesas nos dois processos. A AEPD suportará as suas próprias despesas no presente processo de recurso de segunda instância. ”.

interposto pela ClientEarth conjuntamente com a PAN Europe a partir da afirmação de que o Tribunal Geral não respeitou o princípio da proporcionalidade ao não considerar argumentos sobre a divulgação dos dados ser necessária. Contudo, na mesma oportunidade, o Tribunal afastou a alegação trazida pelas Recorrentes sobre a falta de ponderação acerca do direito à transparência e do direito à proteção da vida privada e dos dados pessoais, ao reforçar que o direito à transparência não prevalece automaticamente em casos envolvendo proteção de dados pessoais²⁶⁴.

Os processos T-493/14²⁶⁵, T-343/13²⁶⁶, C-127/13 P²⁶⁷ e T-115/13 versam sobre o tratamento de dados pessoais por instituições públicas, o qual tem as regras definidas em outras normativas que não a RGPD, como, por exemplo, o Regulamento (CE) n° 45/2001²⁶⁸. O primeiro processo trata de recurso que foi julgado inadmissível. A segunda ação foi julgada improcedente por não restar caracterizado o nexo de causalidade entre o ilícito e o dano. O terceiro cuida do caso de um cidadão alemão solicitando acesso a documentos da Comissão Europeia. O último processo tem por objeto a tentativa de um cidadão em ter acesso a todos os documentos que diziam respeito ao regime complementar dos membros do Parlamento, mas que não lhe foi disponibilizada a lista de membros que participaram de tal regime. Todos esses casos foram resolvidos com base nas previsões do referido Regulamento (CE) n° 45/2001.

²⁶⁴ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-615/13 P, 16 de julho de 2015. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=165906&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1326493>>. Acesso em abril de 2019.

²⁶⁵ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Primeira Seção), caso T-493/14, 17 de fevereiro de 2017. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=187964&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1330669>>. Acesso em abril de 2019.

²⁶⁶ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Sexta Seção), caso T-343/13, 03 de dezembro de 2015. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=172543&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1330669>>. Acesso em abril de 2019.

²⁶⁷ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-127-13 P, 02 de outubro de 2014. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=158192&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1330669>>. Acesso em abril de 2019.

²⁶⁸ Regulamento (CE) n° 45/2001 do Parlamento Europeu e do Conselho de 18 de dezembro de 2000. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, 12 de janeiro de 2001.

Os autos de número C-536/15²⁶⁹ também são regidos por outras legislações diferentes da RGPD, quais sejam, a Diretiva 2002/22/CE²⁷⁰ e a Diretiva 2002/58/CE²⁷¹. Resumidamente, o caso dispõe sobre a possibilidade de uma empresa situada em outro Estado-membro fornecer os dados de seus assinantes a outra empresa “para efeitos da prestação de serviços de informações telefônicas acessíveis ao público e de listas telefônicas” em diversos Estados-membro. A primeira Diretiva mencionada define que a empresa de prestação de serviços é obrigada a pedir consentimento dos seus assinantes para a utilização de seus dados e foi aplicada ao caso.

Já o processo C-235/14²⁷² versa sobre a prevenção à lavagem de dinheiro e de financiamento do terrorismo, com base na interpretação das Diretivas 2005/60/CE²⁷³ e 2007/64/CE²⁷⁴. Nesse processo fica claro a tentativa legislativa de adotar medidas rigorosas para evitar ao máximo práticas ilícitas, em destaque as referentes ao sistema financeiro. Para tanto, medidas relacionadas a proteção de dados são praticadas por Estados-membro, mas esse processo não ajuda na interpretação do que pode caracterizar legítimo interesse nos termos da RGPD/LGPD.

Os autos apensos de numeração C-141/12 e C-372/12²⁷⁵ tratam de pedidos de acesso a minutas oficiais de documentos utilizados na decisão para concessão de visto de imigrantes. O Tribunal definiu que os dados relativos aos processos caracterizavam dados pessoais, contudo, afirmou que, para assegurar o direito de acesso aos dados, garantia fornecida ao titular, seria necessária somente a disponibilização aos titulares de uma “descrição completa desses dados

²⁶⁹ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-536/15, 15 de março de 2017. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=188908&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1330669>>.

²⁷⁰ Diretiva 2002/22/CE, do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrônicas. Jornal Oficial das Comunidades Europeias, 24 de abril de 2002.

²⁷¹ Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. Jornal Oficial das Comunidades Europeias, 31 de julho de 2002.

²⁷² TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Quinta Seção), caso C-235/14, 10 de março de 2016. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=174929&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1330669>>. Acesso em abril de 2019.

²⁷³ Diretiva 2005/60/CE, do Parlamento Europeu e do Conselho, de 26 de outubro de 2005, relativa à prevenção da utilização do sistema financeiro para efeitos de “branqueamento de capitais” e de financiamento do terrorismo. Jornal Oficial da União Europeia, 31 de novembro de 2005.

²⁷⁴ Diretiva 2007/64/CE, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno. Jornal Oficial da União Europeia, 05 de dezembro de 2007.

²⁷⁵ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Terceira Seção), casos: C-141/12 e C-372/12 (apensos), 17 de julho de 2014. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=155114&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=1347230>>. Acesso em abril de 2019.

sob forma inteligível”, o que já asseguraria os direitos oriundos da obtenção dos dados, como, por exemplo, o direito de retificação ou de atualização.

O processo C-73/16²⁷⁶ definiu que o tratamento de dados pessoais feito pela Direção de Finanças da República Eslovaca em parceria com o Serviço de Luta contra a Criminalidade Financeira - Eslováquia ocorre a partir da base legal prevista no artigo 7, alínea ‘e’ da Diretiva 95/46/CE, ou seja, visa a alcançar finalidades de interesse público - base legal prevista nesse dispositivo. O tratamento dos dados resultou na criação de uma lista de sujeitos que ocupam cargos diretivos fictícios a fim de possibilitar a “cobrança de impostos” e a “luta contra a fraude fiscal”.

No caso T-483/13²⁷⁷ se discutiu o descumprimento de cláusulas da Regulamentação 45/2001 pela *European Anti-Fraud Office* (OLAF) ao investigar supostas ações de fraude de um dos seus prestadores de serviço. O caso foi encerrado porque não foi possível demonstrar nexo causal entre o descumprimento do Artigo 25(1) da Regulação mencionada e qualquer dano sofrido pelo autor da ação.

Por fim, o caso C-424/15²⁷⁸ versa sobre dois cidadãos que alegam ilegalidades sobre suas exonerações de funções públicas. Tal fato teria ocorrido devido à fusão de autoridades reguladoras espanholas. A partir da interpretação da Diretiva 2002/21/CE, o TJUE definiu que não haveria nenhuma irregularidade em fundir essas instituições. Contudo, para possibilitar a exoneração do presidente e/ou do administrador com mandatos ainda em curso, decidiu que é necessária a existência de previsões na legislação nacional, que somente a Diretiva não é suficiente para justificar tal ação.

²⁷⁶ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-73/16, 27 de setembro de 2017. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=195046&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=3404080>>. Acesso em abril de 2019.

²⁷⁷ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Quarta Seção), caso T-483/13, 20 de julho de 2016. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=181868&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3404080>>. Acesso em abril de 2019.

²⁷⁸ TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Segunda Seção), caso C-424/15, 19 de outubro de 2016. Disponível em: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184670&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=3404080>>. Acesso em abril de 2019.

CONCLUSÃO

A necessidade de normas gerais sobre proteção de dados se mostra de extrema importância para o contexto atual, em que dados pessoais se misturam com conceitos como a privacidade e o desenvolvimento comercial. É possível verificar desenvolvimento semelhante entre as gerações das normas de proteção de dados pessoais, o que culminou em dois modelos paradigmáticos de proteção: o europeu e o americano.

A norma brasileira, promulgada em 2018, se aproxima bastante da legislação europeia no que tange às bases legais que possibilitam a proteção de dados, principalmente no que se refere à previsão do legítimo interesse do controlador como forma de possibilitar o processamento das informações pessoais, desde que haja proporcionalidade entre as consequências do tratamento para o titular dos dados e o legítimo interesse.

Para se certificar de que há tal verificação de proporcionalidade anterior ao próprio tratamento, a legislação brasileira prevê a necessidade da manutenção de um relatório de impactos do processamento em questão, que poderá ser solicitado a qualquer momento pela ANPD, em especial quando o tratamento for realizado a partir da alegação de configuração do legítimo interesse do controlador. Previsões semelhantes existem no regulamento europeu, e, por isso, acredita-se que trabalhos já feitos sobre esse tema na jurisdição europeia auxiliem a compreensão do que deverá ser feito em âmbito nacional.

A partir dessa compreensão, foi possível alcançar uma sintetização da maneira em que poderá ser confeccionado o relatório de impactos de forma bastante conservadora, o que é positivo e traz seguranças tanto para o titular quanto para o controlador dos dados pessoais.

Contudo, mesmo existindo tal previsão, ainda não há certezas absolutas sobre como e quando o legítimo interesse será efetivamente caracterizado, por isso e devido à falta de jurisprudência nacional sobre o tema, seguiu-se a análise qualitativa da jurisprudência do TJUE sobre o tema nos últimos cinco anos. Esse recorte temporal foi justificado porque tanto a Diretiva 95/46/CE, vigente até 2018, quanto o Regulamento Geral – RGPD, vigente a partir de maio de 2018, trazem previsões semelhantes sobre o legítimo interesse e a necessidade de haver proporcionalidade entre o tratamento de dados realizados a partir dessas bases legais e as consequências para o titular dos dados.

O presente trabalho, através desse exame, logrou observar hipóteses em que existem precedentes tímidos sobre situações em que há a caracterização do legítimo interesse do controlador, se moldando nas hipóteses abordadas pela doutrina, quais sejam: liberdade de

expressão; finalidades históricas, estatísticas ou científicas; segurança; segurança da informação; riscos do negócio; reivindicações legais; e marketing.

Contudo, outras hipóteses não foram caracterizadas em nenhum dos precedentes analisados: envio de mensagens comerciais não desejadas; políticas de denúncias internas; monitoramento de empregados; impedimento de fraudes; e viabilização de pesquisas. Essa não caracterização pode ser justificada pela existência de precedentes anteriores ou mesmo pela falta de persecução de direitos relacionados ao tema pelos titulares dos dados. Então, a falta de precedentes sobre essas hipóteses doutrinárias não impede que tais situações efetivamente caracterizem o interesse legítimo do controlador, principalmente se os passos para a confecção do relatório de dados forem seguidos.

Cabe agora analisar as decisões de autoridades estrangeiras, principalmente aquelas como às submetidas ao Regulamento europeu, com previsões semelhantes à legislação nacional, para que se possa desenhar melhores práticas, mas respeitando os padrões de proteção. Dessa forma, o Brasil poderá ser considerado adequado para transmissão de dados internacionalmente.

Além disso, se mostra de extrema relevância o acompanhamento das orientações e decisões da futura autoridade nacional sobre o tema. É possível que a autoridade crie precedentes mais robustos e que formem guias para o comportamento dos controladores, o que pode gerar maior proteção também para os titulares e, fomentar o tratamento de dados em situações em que esse processamento se mostre útil.

REFERÊNCIAS BIBLIOGRÁFICAS

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Acesso em março de 2019.

BENNETT, Colin; e RAAB, Charles D. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*. 2018. Versão revisada será publicada em "Regulation and Governance". Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972086>. Acesso em 10/06/2019.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2 Reimpr. Rio de Janeiro: Forense, 2019.

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina. 2018.

CUSTERS, Bart; URSIC, Helena. *Worker Privacy in a Digitalized World Under European Law*. 39 Comp. Lam. L. & Pol'y J. 2018. pp. 324-344

DataGuidance by Onetrust; Baptista Luz Advogados. *Comparing privacy laws: GDPR v. LGPD*. 2019. Disponível em: <www.dataguidance.com>. Acesso em maio de 2019.

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

_____. *O Direito Fundamental à Proteção de Dados Pessoais. Direito digital: direito privado e internet*. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. pp. 35-53

FERRETTI, Federico. *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?* Common Market Law Review 51. United Kingdom. 2014. pp. 843-868

INTERNETLAB, Associação Internetlab de Pesquisa em Direito e Tecnologia. *O que está em jogo no debate sobre dados pessoais no Brasil: Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de dados pessoais*. São Paulo. 2016. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Acesso em maio de 2019.

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo, SP: Editora Saraiva, 2011.

LIMBERGER, Têmis. *Informação em Rede: uma Comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu*. Direito digital: direito privado e internet. 2ª ed. Indaiatuba, SP: Editora Foco, 2019. pp. 253-266.

MAJCHER, Klaudia. *E-Commerce in the EU: Searching for Coherence of Data Protection and Competition Law in the Context of Geo-Blocking*. 24 Colum. J. Eur. L.. 2018. pp. 577-595.

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; e DONEDA, Danilo. *Comentário à Nova Lei de Proteção de Dados Pessoais (Lei 13.709/2018): o Novo Paradigma da Proteção de Dados no Brasil*. Revista de Direito do Consumidor, vol. 120. 2018. Pp. 555-587.

_____. *Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120. 2018. Pp. 469-483.

NAUWELAERTS, Wim. *GDPR - The Perfect Privacy Storm: You can Run from the Regulator, but You Cannot Hide from the Consumer*. 3 Eur. Data Prot. L. Rev. 2017. pp. 251-256.

PATERSON, Moira; MCDONAGH, Maeve. *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*. 44 Monash U. L. Rev. 1. 2018. pp. 1-31.

RODOTÀ, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHWABE, Jürgen. *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Organização e Introdução de Leonardo Martins. Tradução de Beatriz Henning, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Gerales Ferreira. Uruguay: Konrad-Adenauer-Stiftung E.V. 2005.