

**UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL  
FACULDADE DE DIREITO  
DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL**

**Clara Affeld Martins de Lima**

**O TRATAMENTO DE DADOS PESSOAIS PELO “LEGÍTIMO INTERESSE” DO  
CONTROLADOR: análise da perspectiva europeia e brasileira**

**Porto Alegre**

**2019**

CLARA AFFELD MARTINS DE LIMA

**O TRATAMENTO DE DADOS PESSOAIS PELO “LEGÍTIMO INTERESSE” DO  
CONTROLADOR: análise da perspectiva europeia e brasileira**

Trabalho de Conclusão de Curso apresentado ao curso de Ciências Jurídicas e Sociais da Universidade Federal do Rio Grande do Sul, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientadora: Prof. Dra. Lisiane Feiten Wingert Ody

Porto Alegre

2019

CLARA AFFELD MARTINS DE LIMA

**O TRATAMENTO DE DADOS PESSOAIS PELO “LEGÍTIMO INTERESSE” DO  
CONTROLADOR: análise da perspectiva europeia e brasileira**

Trabalho de Conclusão de Curso apresentado ao curso de Ciências Jurídicas e Sociais da Universidade Federal do Rio Grande do Sul, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Aprovado em \_\_ de \_\_\_\_\_ de 2019.

**BANCA EXAMINADORA**

---

Prof. Dra. Lisiane Feiten Wingert Ody

Universidade Federal do Rio Grande do Sul

---

Prof. Dra. Kelly Lissandra Bruch

Universidade Federal do Rio Grande do Sul

---

Prof. Me. Rodrigo Ustárroz Cantali

Universidade Federal do Rio Grande do Sul

## **AGRADECIMENTOS**

Agradeço, antes de tudo, aos meus maiores exemplos de caráter e integridade: minha família. Obrigada é pouco para tudo que vocês significam para mim.

À minha orientadora e amiga, Lisiane, pelo atento e constante apoio não só ao longo do desenvolvimento deste trabalho, como também da minha trajetória acadêmica.

Ao Vitor, pelo amor, paciência e por ser meu incansável apoiador em tudo que faço. Obrigada por tanto.

Aos colegas do Silveiro Advogados, pela inspiração diária e pela constante contribuição para minha formação acadêmica, profissional e pessoal.

Às minhas amigas e aos meus amigos, todos, por serem uma família para mim. A felicidade só é real quando compartilhada, e sou verdadeiramente feliz porque sei que posso dividir minha vida com vocês. Obrigada por cada risada, cada conversa, cada experiência.

“The choices we make about how we manage data will be as important as the decisions about managing land during the agricultural age and managing industry during the industrial age. We have a short window of time - just a few years, I think - before a set of norms set in that will be nearly impossible to reverse. Let’s hope humans accept the responsibility for making these decisions and don’t leave it to the machines”.

– Alec Ross, *The Industries of the Future*.

## RESUMO

Vistos como o “novo petróleo”, os dados pessoais são, hoje, insumos essenciais para grande parte das atividades econômicas, o que justifica a crescente preocupação dos ordenamentos jurídicos com a proteção destes ativos. Neste contexto de necessidade de uma sistematização da proteção de dados, tanto a União Europeia, por meio do *General Data Protection Regulation*, quanto o Brasil, por meio da Lei Geral de Proteção de Dados (Lei 13.709/2018), criaram ferramentas jurídicas com a finalidade exclusiva de fortalecer e harmonizar o nível de proteção de dados dos cidadãos. Dentre as muitas semelhanças existentes entre tais legislações, a principal é a previsão de um rol taxativo de fundamentos legais em que o tratamento de dados é considerado lícito. E um destes fundamentos, o “legítimo interesse do controlador”, há muito vem sendo reconhecido como um dos mais complexos e incertos de todas as hipóteses legais para o tratamento lícito de dados pessoais, tanto na Lei brasileira, quanto no Regulamento europeu. Tal complexidade resulta da necessidade de ponderar uma diversidade de fatores para aplicação dessa norma e da ausência de subsídios concretos que orientem sua aplicação. Assim, tendo em vista o caráter aberto da hipótese legal do legítimo interesse do controlador, o presente trabalho tem por objetivo contribuir para a delimitação da amplitude do legítimo interesse como fundamento lícito de tratamento de dados pessoais, através da análise do desenvolvimento desta hipótese legal na União Europeia e no Brasil.

**Palavras-chave:** Proteção de dados pessoais. Tratamento de dados pessoais. Legítimo Interesse. Lei Geral de Proteção de Dados. General Data Protection Regulation.

## **ABSTRACT**

*Over the last couple of years, data has become a valuable asset and is even called the “new oil”, which justifies the growing concern of the legal systems on this subject. In this context, both the European Union and Brazil have created data protection regulations to further harmonize the rules for data protection and to raise the level of privacy for the affected individuals. Among the similarities between such legislations, the main one is the provision of an exhaustive list of legal grounds in which data processing is considered lawful. One of these legal grounds is the “legitimate interest of the controller”, which has been considered one of the most complex and uncertain of all grounds of lawful processing of personal data, both in Brazil and in the European Union. Such complexity results from the need to consider a diversity of factors and from the absence of concrete considerations that might guide the task of those interpreting or applying this provision. Thus, considering the open nature of the legitimate interest ground in Brazilian law and the development of the matter within the European Union, the present work aims to contribute, to some extent, in the process of delimitation of the legitimate interest as a basis for the lawful processing of personal data.*

**Keywords:** *Data Protection. Processing of Personal Data. Legitimate Interest. Brazilian General Data Protection Law. European General Data Protection Regulation.*

## **LISTA DE ILUSTRAÇÕES**

Quadro 1 – Passo-a-passo do "Teste de Ponderação" sugerido pelo GT29 .....	44
Quadro 2 - O Legítimo Interesse na LGPD .....	51

## **LISTA DE ABREVIATURAS E SIGLAS**

CJUE	Corte de Justiça da União Europeia
DPA	Data Protection Authority
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
UE	União Europeia

## SUMÁRIO

	<b>INTRODUÇÃO</b> .....	10
<b>1</b>	<b>O LEGÍTIMO INTERESSE DO CONTROLADOR COMO FUNDAMENTO PARA O TRATAMENTO DE DADOS PESSOAIS NA EUROPA</b> .....	22
1.1	MARCOS LEGAIS .....	22
1.1.1	<b>Diretiva 95/46/CE</b> .....	23
1.1.2	<b>Regulamento Geral de Proteção de Dados</b> .....	24
1.2	JURISPRUDÊNCIA E PRÁTICA .....	28
1.2.1	<b>Casos no âmbito da Corte de Justiça da União Europeia</b> .....	28
1.2.1.1	Caso Rigas .....	28
1.2.1.2	Caso Manni.....	30
1.2.1.3	Caso Ryneš .....	31
1.2.1.4	Caso Google Espanha .....	32
1.2.1.5	Caso ASNEF.....	33
1.2.1.6	Caso Fashion ID .....	34
1.2.2	<b>Casos no âmbito dos Estados-membros da União Europeia</b> .....	35
1.2.2.1	Caso Andbank - Autoridade de Proteção de Dados de Mônaco.....	35
1.2.2.2	Caso Whois - Autoridade de Proteção de Dados da Holanda .....	36
1.2.2.3	Caso Keylogger Software - Justiça Federal do Trabalho da Alemanha .....	37
1.2.2.4	Caso E-commerce - Autoridade de Proteção de Dados da França .....	38
1.2.3	<b>O teste de ponderação/proporcionalidade</b> .....	39
<b>2</b>	<b>O LEGÍTIMO INTERESSE DO CONTROLADOR COMO FUNDAMENTO PARA O TRATAMENTO DE DADOS PESSOAIS NO BRASIL</b> .....	45
2.1	MARCO LEGAL: A LGPD .....	45
2.2	SUBSÍDIOS À APLICAÇÃO DO LEGÍTIMO INTERESSE NO BRASIL.....	48
	<b>CONSIDERAÇÕES FINAIS</b> .....	52
	<b>REFERÊNCIAS</b> .....	55

## INTRODUÇÃO

A intromissão de terceiros e do Estado na vida privada de indivíduos tem sido pauta de discussões há muitos anos. A vida tornou-se cada vez mais conveniente com o uso de tecnologias, e, conseqüentemente, o fluxo de informações pessoais pela rede cresce exponencialmente. Em razão desse cenário, nota-se cada vez mais a necessidade de se gerar mecanismos jurídicos voltados à proteção de dados pessoais e à garantia de autonomia dos indivíduos sobre as suas próprias informações.

Tal preocupação aumenta a passos largos na medida em que os dados pessoais se tornam um elemento estratégico nos novos modelos de negócios, principalmente pela utilidade para diversos fins comerciais. A revista londrina *The Economist*, por exemplo, recentemente divulgou em sua capa que o recurso mais valioso do mundo não é mais o petróleo, mas sim os dados<sup>1</sup>. Em outras palavras, é cada vez mais evidente como a associação entre a tecnologia e o processamento de dados é algo quase essencial no cotidiano de grande parte da população, o que confere um poderio acentuado àqueles agentes que detém o controle sobre esses ativos - o que é um risco apenas recentemente notado pelo ordenamento jurídico.

Nesse cenário, as operações de tratamento de dados<sup>2</sup> dos atuais negócios trazem consigo novos desafios à comunidade jurídica, tendo em vista que, a depender de seu uso - legítimo ou não - inúmeros são os riscos que os titulares<sup>3</sup> podem estar sendo submetidos - como, por exemplo, a exposição indesejada, a restrição à liberdade e a discriminação.

Assim, a proteção de dados pessoais figura como uma disciplina que visa a tutelar a privacidade dos cidadãos, garantindo aos indivíduos a chamada "autodeterminação

---

<sup>1</sup> THE ECONOMIST. Londres: The Economist Group. **The world's most valuable resource is no longer oil, but data**. 6 de maio de 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 10 set. 2019.

<sup>2</sup> O artigo 5, X, da Lei Geral de Proteção de Dados assim define "tratamento de dados": "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: [www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm). Acesso em: 20 ago. 2019.

<sup>3</sup> Assim define a Lei Geral de Proteção de Dados (Lei 13.709/2018) em seu artigo 5º, V, o conceito de titular: "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". Ou seja, o titular pode ser qualquer pessoa física que tenha seus dados pessoais tratados. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: [www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm). Acesso em: 20 ago. 2019.

informativa", que seria o direito do indivíduo decidir acerca da divulgação e uso de seus dados pessoais<sup>4</sup>.

Para introduzir a temática de proteção de dados e estabelecer os conceitos básicos e necessários para a compreensão da análise proposta no presente trabalho, nas próximas linhas serão explorados o desenvolvimento histórico da temática da proteção de dados no Brasil e na União Europeia – onde o desenvolvimento da matéria foi mais precoce<sup>5</sup> – e os princípios que fundamentam ambas essas tradições jurídicas.

No contexto europeu, existem alguns grandes marcos jurídicos que contribuíram para a disseminação e evolução do conceito de privacidade e proteção de dados pessoais. As primeiras leis abordando a temática (chamadas de primeira geração de normas de proteção de dados pessoais) foram as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977)<sup>6</sup>. Nos Estados Unidos, no mesmo período surgiu o *Fair Credit Reporting Act* (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o *Privacy Act* (1974), aplicável à administração pública estadunidense. Nos debates doutrinários, o tema de proteção de dados foi inaugurado a partir da tese de Colin Bennet<sup>7</sup>, de 1992, na qual o autor percebeu um padrão e uma convergência<sup>8</sup> entre os princípios de proteção de dados no sistema americano e europeu.

---

<sup>4</sup> MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang. **Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2015. (Série Direito, Inovação e Tecnologia, v. 1). E-book.

<sup>5</sup> Segundo FERRETTI, a priorização da proteção de dados e o desenvolvimento precoce do assunto na União Europeia foi fortemente influenciado pelos regimes totalitários do século XX, que teriam estimulado as nações a criarem mecanismos para garantir o direito à privacidade aos seus cidadãos. A título exemplificativo, a primeira lei moderna de proteção de dados (a Lei do estado de Hesse, na Alemanha) datada de 1970, foi amplamente motivada pelo crescente desenvolvimento dos sistemas de tecnologia da informação combinados ao medo da população em experimentar, novamente, os abusos vulgarizados no Terceiro Reich: "These experiences demonstrated how easily privacy could be abused, and revealed the extreme consequences of such violations". Outro motivo apresentado pelo autor foi o crescente tráfego de informações pessoais dentro do bloco da União Europeia. FERRETTI, Federico. Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? **Common Law Market Review** 51, 2014, p. 843-868.

<sup>6</sup> MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor** v. 79/2011, p. 45–81, jul. 2011.

<sup>7</sup> BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Ithaca: **Cornell University Press**, 1992, p. 95 a 115. A análise comparativa realizada por Bennett envolve os seguintes países: Estados Unidos, Alemanha, Grã-Bretanha e Suécia.

<sup>8</sup> Segundo Bennett: "Convergência significa mais que similaridade. Denota um padrão que ultrapassa o tempo, um processo dinâmico, ao invés de uma condição estática. [...] Deste modo, a partir de uma posição em que os Estados não tinham nenhuma ou muito pouca legislação de proteção de dados e, por isso, havia diversos tipos de estratégia para o tema, um consenso emergiu durante a década de 1970, em volta de princípios. Podemos concluir, portanto,

Com o desenvolvimento do tema e a partir de tais regulamentos, surgiram, com o tempo, importantes instrumentos internacionais e transnacionais que contribuíram para a consolidação de um conceito de privacidade ligado à proteção de dados pessoais. No contexto da União Europeia, destacam-se a Convenção 108 do Conselho da Europa (1981), as Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais (1980)<sup>9</sup>, a Diretiva Europeia 95/46/CE relativa à proteção de dados pessoais (1995) e o mais novo Regulamento Geral de Proteção de Dados da União Europeia, o GDPR<sup>10</sup> (2018), que serão abordados a seguir.

O grau de atenção à proteção de dados entre tais documentos é, naturalmente, variável. Contudo, todas as normativas citadas declaram que o processamento de informações pessoais deve ser (i) obtido de forma justa e lícita; (ii) com respeito ao propósito original do tratamento; (iii) adequado, relevante e não excessivo em relação ao propósito do tratamento; (iv) atualizado, devendo refletir a situação atual do indivíduo; (v) acessível ao titular do dado; (vi) mantido seguro e (vii) eliminado após o atingimento da finalidade<sup>11</sup>. Como se verá mais adiante na presente introdução, tais parâmetros muito se relacionam com a evolução do que veio a se chamar de princípios gerais da proteção de dados.

Contudo, antes de adentrar em cada regulamento específico, vale enfatizar outro importante marco no desenvolvimento do conceito de privacidade e proteção de dados na UE: o julgamento do caso da Lei do Censo (*Volkszählungsgesetz*)<sup>12</sup> pelo Tribunal Constitucional Alemão em 15 de dezembro de 1983.

---

que a convergência ocorreu.” BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Ithaca: **Cornell University Press**, 1992, p. 111 e 112.

<sup>9</sup> Segundo DAVIES e BANISAR, as regras contidas nesses dois primeiros documentos formam o núcleo das leis de proteção de dados de dezenas de países ao redor do mundo. BANISAR, David. DAVIES, Simon. *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, And Surveillance Laws and Developments*. **The John Marshall Journal of Computer & Information Law**, 1999. p. 11.

<sup>10</sup> A sigla em inglês que se destaca nas discussões acadêmicas e nos quadros internacionais é GDPR, correspondente à "General Data Protection Regulation". Por essa razão, será essa a sigla adotada por este trabalho. Em português, a sigla corresponde à RGPD - Regulamento Geral de Proteção de Dados. UNIÃO EUROPEIA. Regulamento (UE) n° 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 04/05/2016. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 20 set. 2019.

<sup>11</sup> BANISAR, David. DAVIES, Simon. *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, And Surveillance Laws and Developments*. **The John Marshall Journal of Computer & Information Law**, 1999. p. 11.

<sup>12</sup> Segundo Laura Schertel Mendes, "A lei do recenseamento visava à coleta dos dados dos cidadãos referentes à profissão, moradia e local de trabalho, com intuito de fornecer à administração pública informações acerca do crescimento populacional, da distribuição espacial da população pelo território e das atividades econômicas

Nesse julgamento histórico, o Tribunal alemão reconheceu, por unanimidade, o *Recht auf Informationelle Selbstbestimmung* (Direito à Autodeterminação Informativa), que viria a influenciar todo o desenvolvimento da disciplina de proteção de dados não só no Estado alemão, como em toda a União Europeia. O Tribunal estabeleceu que o direito à autodeterminação informacional pressupõe que, mesmo sob as condições da moderna tecnologia de processamento de informações, o indivíduo exerça sua liberdade de decisão sobre as ações a serem precedidas ou omitidas em relação aos seus próprios dados. Nesse sentido, conforme ensina Laura Schertel Mendes:

A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subseqüentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo à protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação<sup>13</sup>.

Assim, a Corte reconheceu uma carga participativa dos titulares muito maior que a garantida pela experiência jurídica em períodos anteriores: os indivíduos passaram a ser os verdadeiros donos de seus dados. Dessa forma, a participação do indivíduo no tratamento de dados pessoais passa a ser vista como um envolvimento contínuo em todo o processo, desde a coleta ao armazenamento<sup>14</sup>. Nesse sentido, Maria Claudia Cachapuz ensina que o reconhecimento da autodeterminação informativa implicou na consequência de que "toda e

---

realizadas no país. Os dados a serem coletados por pesquisadores estavam listados na lei, que estabelecia também uma multa para o cidadão que se recusasse a responder. Ademais, o § 9.º da norma determinava que os dados poderiam ser comparados àqueles presentes em registros públicos, com a finalidade de averiguar a veracidade das informações fornecidas, além de possibilitar a sua transmissão na forma anônima a órgãos públicos federais. Foram ajuizadas diretamente diversas reclamações constitucionais contra a lei do recenseamento, com fundamento na violação direta ao Art. 2 I GG, que protege o livre desenvolvimento da personalidade. O Tribunal conheceu da reclamação e, no mérito, confirmou a constitucionalidade da lei em geral, declarando nulos os dispositivos que determinavam a comparação dos dados coletados, bem como a sua transferência para outros órgãos da administração". MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79, p. 45-82, jul./set. 2011.

<sup>13</sup> MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor v. 79/2011**, p. 45–81, jul. 2011.

<sup>14</sup> MAYER-SCHÖNBERGER, Victor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: **The Mit Press**, 2001.

qualquer informação pessoal só se tornasse pública se tutelada por um determinado interesse público, porque conhecida do titular a sua existência e com quem é compartilhada"<sup>15</sup>.

Retornando aos instrumentos europeus que moldaram a disciplina de proteção de dados, um dos principais marcos normativos que elevou a proteção de dados como direito fundamental foi a Convenção nº 108 do Conselho da Europa, de 1981<sup>16</sup>. A denominada "Convenção para Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal" tinha por objetivo garantir a toda pessoa, independente de nacionalidade, o respeito aos direitos e liberdades fundamentais, especialmente ao direito à vida privada em relação ao tratamento dos dados pessoais<sup>17</sup>.

Muito embora a Convenção nº 108 tenha promovido um relevante avanço no contexto regulatório da proteção de dados, ela ainda possuía falhas na sua efetividade. Tatiana Malta Vieira menciona dois motivos que possivelmente ocasionaram tais falhas: (i) a ratificação do documento por apenas alguns Estados-membros da UE, o que dificultava a harmonização legislativa no bloco europeu; e (ii) o carácter de *non self-executing* do documento, que dependia de frequentes remissões aos direitos nacionais, o que nem sempre ocorria pois nem todos os países signatários dispunham de legislação específica a respeito da matéria<sup>18</sup>.

Outro marco relevante foi a publicação, em 1980, das Diretrizes relativas à política internacional de proteção da privacidade e dos fluxos transfronteiriços de dados pessoais pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE). As diretrizes abordaram padrões mínimos para a proteção da privacidade e liberdade individual, como, por exemplo, os princípios da limitação da coleta de dados, da qualidade dos dados, da finalidade, da limitação de utilização, do back-up de segurança, da abertura, da participação do indivíduo

---

<sup>15</sup> CACHAPUZ, Maria Cláudia Mércio. Privacidade, proteção de dados e autodeterminação informativa. **Revista Jurídica da Presidência**, Brasília, DF, v. 15. n. 107, p. 823-848, out. 2013/jan. 2014.

<sup>16</sup> BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília, DF: ENDC, 2010. (Caderno de Investigações Científicas, v. 2). Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-deprotecao-de-dados-pessoais.pdf>. Acesso em: 25 out. 2019. p. 47.

<sup>17</sup> Artigo 1º da Convenção 108 do Conselho da Europa: "A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»)." UNIÃO EUROPEIA. Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal: **Conselho da Europa**, Estrasburgo, 28 jan. 1981. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 10 out. 2019.

<sup>18</sup> VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. 2007. Dissertação (Mestrado em Direito, Estado e Sociedade) – Faculdade de Direito, Universidade de Brasília, Brasília, DF, 2007. Disponível em: [repositorio.unb.br/bitstream/10482/3358/1/2007\\_TatianaMaltaVieira.pdf](http://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf). Acesso em: 12 out. 2019.

e da responsabilização<sup>19</sup>. Contudo, assim como ocorreu no caso da Convenção 108 do Conselho da Europa, a ausência de aplicação direta das Diretrizes da OCDE e a falta de especificidade do documento, fez com que sua aplicação - por mais que tenha sido extremamente importante num contexto histórico e de desenvolvimento da matéria de proteção de dados - ainda apresentasse problemas no sentido de sua eficácia.

Assim, na busca de corrigir tal problemática, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho da Europa foi aprovada em 1995, trazendo um novo paradigma de proteção de dados ao contexto europeu. O objetivo central da Diretiva, conforme o seu artigo 1º, era assegurar, dentro dos Estados-membros da UE, "a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais"<sup>20</sup>. Além disso, conforme já destacado anteriormente, tal Diretiva trouxe, pela primeira vez, um rol taxativo de hipóteses em que os dados pessoais podem ser tratados pelos controladores de dados, sendo qualquer tratamento realizado fora de tais hipóteses, considerado ilícito<sup>21</sup>.

Apesar do texto da Diretiva não possuir eficácia direta, devendo o conteúdo ser transposto pelas legislações nacionais dos Estados-membros, seus reflexos são vistos até hoje, principalmente através do Regulamento que a revogou, o GDPR, que é inegavelmente uma evolução da Diretiva 95/46/CE<sup>22</sup>. Nesse sentido, afirma-se que a Diretiva foi um dos principais

---

<sup>19</sup> ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICOS (OCDE). **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais**. 1980. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 25 out. 2019.

<sup>20</sup> "Artigo 1º Objecto da directiva: 1. Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais. 2. Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas à protecção assegurada por força do nº 1." DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**. Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=pt>. Acesso em: 12 out. 2019.

<sup>21</sup> As hipóteses legais de tratamento de dados que constavam no art. 7º da Diretiva de 1995 eram: a) o consentimento do titular, b) o tratamento para fins de execução de contrato, c) o tratamento para fins de obrigação legal, d) a proteção do interesse vital do titular, e) o interesse público e, por fim, a hipótese mais ampla: f) a possibilidade de tratamento em razão de legítimo interesse do responsável pelo tratamento, ponderando-se os interesses, direitos e liberdades fundamentais do titular dos dados. DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**. Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=pt>. Acesso em: 12 out. 2019.

<sup>22</sup> KAMARA, Irene. DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach. **The Cambridge handbook of consumer privacy**. 2018, p. 321-352.

diplomas responsáveis por alçar o direito à proteção de dados pessoais ao *status* de direito fundamental.

Por fim, passando à situação atual do contexto europeu de proteção de dados, no ano de 2016 foi aprovado o *General Data Protection Regulation* (GDPR), que, com sua entrada em vigor em maio de 2018, substituiu a Diretiva 95/46/CE. O Regulamento, conforme seu artigo 1º, "estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" e "defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados"<sup>23</sup>.

Além disso, tal como a Diretiva que o antecede, o Regulamento trouxe, também, em seu artigo 6º, um rol taxativo de seis hipóteses em que o tratamento de dados pode ser considerado lícito, sendo elas: a) o tratamento de dados mediante o consentimento do titular; b) quando o tratamento for necessário para a execução de um contrato; c) quando o tratamento for necessário para o cumprimento de uma obrigação legal; d) para a defesa dos interesses vitais do titular ou outra pessoa singular; e) para atender às funções do interesse público ou exercício de autoridade pública; e, por fim, f) quando o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros<sup>24</sup>.

No contexto brasileiro, em contrapartida ao pioneirismo europeu na matéria, a primeira lei dedicada exclusivamente à proteção de dados foi sancionada em 14 de agosto de 2018, quase vinte e cinco anos após a publicação da Diretiva do bloco europeu.

Assim, a Lei Geral de Proteção de Dados – Lei 13.709/2018 ou “LGPD”, como é conhecida - inaugurou um regime legal de proteção de dados pessoais no país e colocou o Brasil no seleto rol de países que possuem legislações específicas voltadas à proteção de dados.

Segundo Laura Schertel Mendes e Danilo Doneda:

---

<sup>23</sup> UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD) 2015/679/CE**, de 27 de abril de 2016. Disponível em: <<https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 20 out. 2019.

<sup>24</sup> “Artigo 6 (1) O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; 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; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; 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”. UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD) 2015/679/CE**, de 27 de abril de 2016. Disponível em: <<https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 20 out. 2019.

A referida Lei vem complementar o marco regulatório brasileiro da Sociedade da Informação ao compor, juntamente com a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor, o conjunto normativo que moderniza o tratamento da informação no Brasil. Seu objetivo é proporcionar garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor<sup>25</sup>.

Quanto às principais influências que moldaram a LGPD, é possível verificar que a legislação brasileira se inspira, primeiramente, no modelo europeu de proteção de dados<sup>26</sup>, possuindo inegáveis semelhanças com o GDPR europeu. Essa influência pode ser percebida tanto na exigência de uma base legal para o tratamento de dados, quanto nos princípios gerais, nas regras especiais para o tratamento de dados sensíveis e na previsão de criação de uma autoridade nacional de proteção de dados para garantir a aplicação da lei – a “ANPD”.

No entanto, apesar da influência europeia, ainda se nota a clara influência da tradição legislativa brasileira nas normas da LGPD, que acabam por distanciar - ainda que suavemente - a LGPD do GDPR. Do Marco Civil da Internet, por exemplo, há o art. 2º, que enumera os fundamentos da proteção de dados no Brasil, muito similares aos citados no Marco Civil<sup>27</sup>.

Da Lei do Cadastro Positivo, observa-se a regra relativa à revisão das decisões automatizadas (art. 5º, VI, da Lei 12.414/2011), conceito desenvolvido anteriormente pela Diretiva 46/95/CE do bloco europeu, mas que foi introduzido pela primeira vez no ordenamento brasileiro através da Lei do Cadastro Positivo como um direito à revisão<sup>28</sup>.

Do Código do Consumidor (CDC), nota-se a influência do diálogo das fontes e do art. 7º do CDC ao art. 64 da LGPD, que estabelece que os direitos e princípios expressos na Lei “não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte”. Segundo Laura Schertel Mendes e Danilo Doneda, “tal dispositivo visa consolidar na disciplina da proteção de dados a aplicação harmônica e coordenada de normas de um sistema jurídico, expressa no conceito de diálogo das fontes, formulado por Cláudia Lima Marques”<sup>29</sup>. Além disso, de

---

<sup>25</sup> DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 120/2018. p. 469-483.

<sup>26</sup> DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 120/2018. p. 469-483.

<sup>27</sup> DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 120/2018. p. 469-483.

<sup>28</sup> DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 120/2018. p. 469-483.

<sup>29</sup> MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**. vol. 1009/2019. 2019. p. 2.

influências do Código do Consumidor também se notam algumas regras de responsabilidade, em especial a inversão do ônus da prova, as excludentes de responsabilidade, a possibilidade de danos coletivos, assim como o conceito de tratamento impróprio de dados (art. 42, §§ 2º e 3º, 43 e 44, da LGPD)<sup>30</sup>. Ou seja, é possível observar que mesmo que a LGPD seja inegavelmente inspirada no modelo europeu de proteção de dados, ela ainda assim interage com a legislação e cultura jurídica brasileira.

Tal como a legislação europeia atual de proteção de dados, a LGPD traz em seu artigo 7º um rol taxativo de dez hipóteses em que os dados podem ser tratados de maneira lícita, sendo elas: a) mediante o consentimento expresso do titular; b) para o cumprimento de obrigação legal ou regulatória pelo controlador; c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; d) para a realização de estudos por órgãos de pesquisa; e) para a execução de contrato ou procedimentos preliminares a este; f) para o exercício regular de direitos em processo judicial; g) para a proteção da vida ou incolumidade física; h) para a tutela da saúde; i) quando necessário para atender aos interesses legítimos do controlador; j) para a proteção do crédito<sup>31</sup>.

Muito embora existam certas diferenças entre os regulamentos analisados, verdade é que tanto a lei brasileira, quanto o regulamento europeu trazem consigo uma série de princípios que guiam e impõem limites ao tratamento de dados, com a finalidade de tutelar o direito à autodeterminação informativa dos titulares<sup>32</sup>.

---

<sup>30</sup> DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 120/2018. p. 469-483.

<sup>31</sup> “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019); IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente” BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: [www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm). Acesso em: 20 out. 2019.

<sup>32</sup> MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 68.

O conjunto destes princípios é conhecido como "*Fair Information Principles*", e sua origem remonta à década de 1970. Aliás, como ensina Laura Schertel Mendes, “mesmo os ordenamentos jurídicos mais diversos preveem praticamente os mesmos princípios de proteção de dados, com mínimas diferenças”, sendo possível afirmar a existência de uma convergência internacional sobre o tema<sup>33</sup>.

Nesse sentido, os cinco princípios de proteção de dados mais citados pela doutrina, e que devem ser observados no momento do tratamento de dados, são: o princípio da finalidade, o princípio da transparência (também chamado de "princípio da publicidade"), o princípio do consentimento, o princípio da qualidade dos dados e o princípio da segurança física e lógica. Nas próximas linhas se abordará, de maneira sucinta, as principais características de cada um desses princípios basilares da matéria de proteção de dados.

O *princípio da finalidade* indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados<sup>34</sup>. Esse princípio também serve para identificar se determinado uso de dados pessoais é adequado e razoável, de acordo com a primeira finalidade informada no momento da coleta<sup>35</sup>. Por fim, esse princípio exige que o responsável pelo tratamento de dados estabeleça de forma expressa e limitada a finalidade específica do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas<sup>36</sup>.

O *princípio da transparência* - ou *princípio da publicidade* - se baseia na ideia de que a transparência é uma das principais maneiras de se combaterem os abusos<sup>37</sup>. Portanto, segundo este princípio, o tratamento de dados não pode ser realizado sem o conhecimento daquele a quem os dados se referem<sup>38</sup>.

Para possibilitar ao titular o controle dos seus dados, outro princípio importante é o *princípio do consentimento*, que apesar de não se aplicar em todas as hipóteses de tratamento de dados (como o legítimo interesse, por exemplo), é de extrema importância pois é a externalização do exercício da liberdade de controle de dados pessoais do indivíduo. Segundo

---

<sup>33</sup> MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 68.

<sup>34</sup> MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor** v. 79/2011, p. 45–81, jul. 2011

<sup>35</sup> DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 216.

<sup>36</sup> MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79/2011, p. 45–81, jul. 2011.

<sup>37</sup> BENNETT, Colin. *Regulating Privacy: data protection and public policy in Europe and the United States*. Ithaca: **Cornell University Press**, 1992, p. 156.

<sup>38</sup> DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 216.

esse princípio, o consentimento deve ser consciente e informado, e apenas situações excepcionais, previstas pela legislação, são capazes de justificar o processamento de dados sem o consentimento prévio do titular do dado pessoal<sup>39</sup>.

Já o *princípio da qualidade dos dados* se refere à exigência de que os dados objeto de tratamento sejam adequados, pertinentes e não excessivos em relação à finalidade declarada, além de serem objetivos, atualizados e exatos<sup>40</sup>. Tal princípio exige a constante atualização das bases de dados, de modo a impedir que os dados referentes aos titulares fiquem ultrapassados. Aqui neste princípio se incluem os direitos de acesso, retificação e cancelamento dos dados<sup>41</sup>.

Por fim, o *princípio da segurança física e lógica* refere-se à necessidade de garantia que os dados pessoais estejam em ambientes protegidos contra extravios, destruições, modificações e desvios não autorizados pelos interessados<sup>42</sup>.

Além dos princípios gerais de proteção de dados, a principal semelhança entre as legislações vigentes na UE e no Brasil é que ambas preveem um rol taxativo de fundamentos legais em que o tratamento de dados é considerado lícito. E dentre estas hipóteses legais, nota-se que outro ponto em comum entre as legislações é o previsto no inciso "f" do artigo 6º do GDPR e o inciso "IX" do artigo 7º da LGPD: a possibilidade de tratamento de dados quando estes forem necessários para o atender aos interesses legítimos do controlador ou de terceiros<sup>43</sup>. Mas, afinal, o que seria esse "interesse legítimo"? É possível estabelecer parâmetros a sua aplicação?

A denominação "interesse legítimo" trata-se de uma redação genérica que deixa uma grande margem de interpretação e que muitas vezes já conduziu à falta de previsibilidade e de segurança jurídica<sup>44</sup>, mesmo na Europa onde ele já é previsto desde 1995. Como era previsível, essa base legal ganhou ainda mais relevância diante do contexto atual de uma economia baseada no uso intensivo de dados, no qual o legítimo interesse ganhou o *status* de praticamente uma

---

<sup>39</sup> MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79/2011, p. 45–81, jul. 2011.

<sup>40</sup> MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79/2011, p. 45–81, jul. 2011.

<sup>41</sup> MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79/2011, p. 45–81, jul. 2011.

<sup>42</sup> DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 217.

<sup>43</sup> Necessário esclarecer que o presente trabalho, como refere o próprio título, se dedica a explorar o legítimo interesse exclusivamente em relação aos controladores diretos do dado pessoal, e não em relação a terceiros.

<sup>44</sup> BALBONI, Paolo. COOPER, Daniel. IMPERIALI, Rosario. MACENAITE, Milda. Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection. **International Data Privacy Law**, 2013. p. 247.

"carta coringa regulatória" para abarcar uma miríade de possíveis usos de dados pessoais<sup>45</sup> e situações raras e imprevistas.

Segundo Marcel Leonardi, ex-diretor do Google Brasil, pesquisas realizadas na Europa demonstram que apenas 5% do tratamento de dados declarados pelas empresas tem como base o consentimento, ao passo que 70% indicam o legítimo interesse<sup>46</sup> para a maioria dos processamentos. Contudo, em contrapartida à vulgarização dessa hipótese legal, se a mesma for utilizada no contexto correto e com a aplicação de critérios adequados, a hipótese de tratamento sob o fundamento do legítimo interesse possui um papel essencial de garantir uma margem de adaptabilidade aos controladores de dados pessoais, de modo a não atravancar os avanços tecnológicos e os novos modelos de negócio.

Sobre a importância da hipótese do legítimo interesse, vale destacar as palavras de Federico Ferretti:

The legitimate interest of data controllers or that of third parties is known as the “balance of interest” clause. Data controllers, especially businesses, can process personal data lawfully without meeting the tight conditions provided in Article 7 from (b) to (e) and, most of all, without the consent of individuals under condition (a) of Article 7. Relying on consent may be burdensome for businesses, especially if applied with the high standards set by the Article 29 Working Party, or strictly as a “clear affirmative action” by data subjects as required by the Proposed Regulation. Moreover, new technologies such as data analytics increasingly use large data sets obtained from diverse unrelated sources (“Big Data”) which make the obtaining of consent impracticable. Therefore, the legitimate interest clause is considered the criterion upon which the majority of personal data processing takes place, at times the default position, especially for commercial transactions<sup>47</sup>.

A presente pesquisa, portanto, visa a analisar, através do método descritivo e exploratório, com uma abordagem comparativa funcional contextualizada, de que modo a hipótese do legítimo interesse vem sendo aplicada e interpretada pela doutrina e jurisprudência europeia, e como tais parâmetros - se existentes - podem servir de orientação à uma efetiva aplicação da Lei Geral de Proteção de Dados no Brasil<sup>48</sup>.

---

<sup>45</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 249.

<sup>46</sup> BERBERET, Lúcia. **“Interesse legítimo” supera “consentimento” no tratamento de dados pessoais pelas empresas**. Disponível em: <<http://www.telesintese.com.br/interesse-legitimo-supera-consentimento-no-tratamento-de-dados-pelas-empresas/>>. Acesso em: 10 set. 2019.

<sup>47</sup> FERRETTI, Federico. Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? **Common Law Market Review** 51, 2014, p. 843-868.

<sup>48</sup> Vale salientar, de início, que a presente pesquisa não sugere a aplicação direta, no Brasil, dos critérios estabelecidos ao legítimo interesse pela experiência europeia, pois parte-se do pressuposto de que tanto a cultura jurídica quanto os padrões de vida no Brasil são diferentes do continente europeu. Assim, o trabalho apenas se

Para tanto, a monografia é dividida em duas partes principais.

A primeira parte explora o desenvolvimento do legítimo interesse no âmbito da UE, desde a sua criação pela Diretiva 95/46/UE em 1995, até a entrada em vigor do GDPR em 2018. Nesse capítulo, são analisados julgados da Corte de Justiça da União Europeia, casos de Tribunais e Autoridades Nacionais de Proteção de Dados dos Estados-membros e estudos doutrinários acerca da evolução e aplicabilidade da hipótese do legítimo interesse.

A segunda e última parte explora o desenvolvimento e conceitualização da hipótese do legítimo interesse do controlador no âmbito da legislação brasileira (LGPD) e quais são os possíveis parâmetros de aplicação no Brasil.

## **1 O LEGÍTIMO INTERESSE DO CONTROLADOR COMO FUNDAMENTO PARA O TRATAMENTO DE DADOS PESSOAIS NA EUROPA**

A hipótese legal de tratamento de dados pelo legítimo interesse do controlador se encontra prevista na União Europeia desde 1995, pela Diretiva 95/46/CE e até hoje ainda consta nas hipóteses previstas no GDPR. Assim, o presente capítulo visa a analisar como se deu o desenvolvimento do legítimo interesse no contexto europeu, tanto na sua dimensão legal, quanto na sua dimensão prática.

A análise da dimensão legal explora quais foram os marcos legais que trouxeram o legítimo interesse como fundamento para o tratamento lícito de dados, e como eram tais disposições.

A análise da dimensão prática, por sua vez, foi baseada em três etapas: em primeiro lugar, a análise de todos julgados envolvendo a questão do legítimo interesse no âmbito da Corte de Justiça da União Europeia (CJUE); em segundo lugar, a análise de alguns casos apreciados em nível nacional pelos estados-membros da UE; e, em terceiro e último lugar, a análise das contribuições doutrinárias sobre a matéria.

### **1.1 MARCOS LEGAIS**

No presente subcapítulo serão analisados dois marcos legais essenciais para o desenvolvimento do legítimo interesse na UE: a Diretiva 95/46/CE de 1995 e o *General Data Protection Regulation* (Regulamento Geral de Proteção de Dados) de 2018.

---

destina a expor o desenvolvimento e o cenário atual da aplicação do legítimo interesse no contexto europeu, para que essa experiência possa servir de orientação e inspiração à nova Lei Geral de Proteção de Dados brasileira.

### 1.1.1 Diretiva 95/46/CE

Na União Europeia, o legítimo interesse apareceu como hipótese de tratamento de dados pela primeira vez no artigo 7, alínea "f" da Diretiva 95/46/CE:

#### Artigo 7º

Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se:

(...)

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.

Contudo, por se tratar de um instrumento normativo que estabelecia objetivos gerais a serem internalizados pelos ordenamentos jurídicos domésticos de cada um dos estados-membros da União Europeia, notou-se, negativamente, que ao longo da vigência da Diretiva houve: (i) ausência de aplicação harmônica de tal base legal no bloco europeu, pois cada país estabeleceu suas próprias regras e leituras distintas acerca do legítimo interesse; e (ii) risco de esvaziamento das demais bases legais para tratamento de dados pessoais, na medida em que o legítimo interesse poderia ser visto como a hipótese menos restritiva que as demais<sup>49</sup>.

Sobre o primeiro ponto, vale ressaltar que logo no primeiro relatório sobre a implementação da Diretiva pelos países da UE<sup>50</sup> realizado em 2003, a Comissão Europeia já indicou que a transposição do art. 7º da Diretiva para as legislações dos Estados-membros foi insatisfatória e divergente. Além da incongruência na implementação da provisão na UE, o interesse legítimo tem sido frequentemente caracterizado como uma "brecha" na proteção de dados pessoais<sup>51</sup>, principalmente porque não se pode verificar se o teste de ponderação acerca da existência ou não de um legítimo interesse (que será analisado no subcapítulo seguinte) realmente foi realizado pelo controlador, a menos que isso seja contestado judicialmente<sup>52</sup>.

<sup>49</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 249.

<sup>50</sup> COMISSÃO EUROPEIA. **Primeiro relatório sobre a implementação da directiva relativa à protecção de dados (95/46/CE)**, COM/2003/0265 final. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52003DC0265&from=EN>>. Acesso em: 27 out. 2019.

<sup>51</sup> KAMARA, Irene. DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach. **The Cambridge handbook of consumer privacy**. 2018, p. 321-352.

<sup>52</sup> BALBONI, Paolo. COOPER, Daniel. IMPERIALI, Rosario. MACENAITE, Milda. Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection. **International Data Privacy Law**, 2013. p. 247.

Quanto às divergências internas na aplicação da Diretiva, destacam-se as palavras de Paul Voigt e Axel von dem Bussche<sup>53</sup>:

The Data Protection Directive did not live up to its objectives and failed to align the level of data protection within the EU. Legal differences arose as a consequence of the implementing acts adopted by the various EU Member States. Data processing activities that were allowed in one EU Member State could be unlawful in another one with regard to the specific execution of data processing.

As críticas à Diretiva também se voltaram à falta de orientações mais específicas acerca da interpretação do legítimo interesse do responsável pelo tratamento - o que posteriormente foi sanado pelo GDPR, eis que o regulamento introduz novos conceitos sobre o interesse legítimo e fornece exemplos de hipóteses de incidência dessa base legal em suas considerações iniciais (“Considerandos”)<sup>54</sup>.

### 1.1.2 Regulamento Geral de Proteção de Dados

Como uma evolução legislativa, o Regulamento Geral da Proteção de Dados (*General Data Protection Regulation*, ou GDPR), entrou em vigor em maio de 2018, após 2 anos de *vacatio legis*, para substituir a antiga Diretiva 95/46/CE, visando a harmonização das leis de proteção de dados dos países da União Europeia.

Vale ressaltar que a natureza de "Regulamento" e não de "Diretiva", como era anteriormente, confere uma garantia de proteção de dados pessoais muito mais homogênea no bloco europeu, visto que o Regulamento possui aplicação direta nos Estados-membros<sup>55</sup>, não precisando ser transposto para as legislações específicas de cada país. A Diretiva, por sua vez, consistia em orientações de como os países membros da UE deveriam formular suas respectivas leis nacionais, havendo, por conseguinte, um grande espaço para interpretações jurídicas divergentes por cada um dos países membros<sup>56</sup>. Já o Regulamento é um mecanismo do direito comunitário europeu com eficácia imediata, sem necessidade de intermediação dos países membros da UE.

---

<sup>53</sup> VOIGT, Paul. BUSSCHE, Axel von dem. The EU General Data Protection Regulation (GDPR): A practical guide. Springer, **Berlin Springer International Publishing Springer**, 2017. p. 2.

<sup>54</sup> KAMARA, Irene. DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach. **The Cambridge handbook of consumer privacy**. 2018, p. 321-352.

<sup>55</sup> VOIGT, Paul. BUSSCHE, Axel von dem. The EU General Data Protection Regulation (GDPR): A practical guide. Springer, **Berlin Springer International Publishing Springer**, 2017. p. 3.

<sup>56</sup> FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. São Paulo: **Revista dos Tribunais**, 2019. p. 804.

Dessa forma, o Regulamento surge com o objetivo de recuperar a confiança dos cidadãos europeus no tratamento responsável dos seus dados pessoais em todo o continente, a fim de impulsionar a economia digital em todo o mercado interno da UE<sup>57</sup>.

Assim, a hipótese de tratamento de dados pessoais do legítimo interesse é fundamentada no artigo 6º, alínea "f", do GDPR:

**Artigo 6º**

1. O tratamento só é lícito na medida em que se verifique pelo menos uma das seguintes situações:

(...)

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.

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

Ao fim e ao cabo, em comparação ao art. 7(f) da anterior Diretiva 95/46/CE, o art. 6(f) não fornece muitos elementos de inovação. Em contrapartida, o viés econômico do mercado motivava a manutenção do interesse legítimo como hipótese de tratamento, tanto pela redução de custos administrativos, quanto também pela necessidade de fomento à inovação, haja vista que a hipótese do legítimo interesse fornece uma margem de liberdade às empresas que tratam dados pessoais.

Em relação à Diretiva que antecede o Regulamento, a redação foi aprimorada em vários aspectos. Uma diferenciação significativa é a desassociação do escopo dos interesses, direitos e liberdades dos titulares de dados que não devem ser ultrapassados, do âmbito material do instrumento jurídico. A hipótese do interesse legítimo no art. 7, f, da Diretiva 95/46/CE fazia referência explícita ao art. 1, nº 1 da Diretiva<sup>58</sup>, vinculando assim a ponderação dos interesses e direitos do titular em relação às suas liberdades e direitos fundamentais, nomeadamente do direito à vida privada. O disposto no art. 6, "f" do GDPR descarta a referência ao assunto e se

---

<sup>57</sup> VOIGT, Paul. BUSSCHE, Axel von dem. The EU General Data Protection Regulation (GDPR): A practical guide. Springer, **Berlin Springer International Publishing Springer**, 2017. p. 2.

<sup>58</sup> O art. 1, nº 1 da Diretiva apenas previa a proteção das liberdades e direitos fundamentais do indivíduo, nomeadamente o direito à vida privada: "Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais". DIRETIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**. Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=pt>. Acesso em: 12 out. 2019.

refere a "os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". A mudança na redação pode ser considerada como uma ampliação do escopo da lei. Quaisquer interesses, direitos e liberdades que mereçam proteção de dados pessoais devem ser avaliados pelo responsável pelo tratamento ao considerar o interesse legítimo em suas atividades de processamento. Outra diferenciação relevante foi a inclusão de um tratamento especial quando os dados forem referentes a crianças, previsão que não constava na Diretiva.

Uma importante evolução do Regulamento em comparação à Diretiva foi a inclusão de “Considerandos” que exemplificam e esclarecem a aplicabilidade do legítimo interesse. Apesar de não definir o que entende por interesses legítimos, o legislador europeu, nas Considerações nº 47<sup>59</sup> e 49<sup>60</sup> do Regulamento, expõe um conjunto variado de exemplos em que a hipótese do

---

<sup>59</sup> Considerando 47, GDPR: "(47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta". UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD) 2015/679/CE**, de 27 de abril de 2016. Disponível em: <<https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 20 out. 2019.

<sup>60</sup> Considerando 49, GDPR: "(49) O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, ou seja, a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança, constitui um interesse legítimo do responsável pelo tratamento. Pode ser esse o caso quando o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas". UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD) 2015/679/CE**, de 27 de abril de 2016. Disponível em: <<https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 20 out. 2019.

legítimo interesse é aplicável: (i) a existência de uma relação prévia entre o responsável e o titular<sup>61</sup>; (ii) a prevenção e o controle de fraudes<sup>62</sup>; (iii) a comercialização direta de bens ou serviços<sup>63</sup>; (iv) a existência de uma relação de grupo empresarial, com necessidade de transmissão de dados para fins administrativos internos<sup>64</sup>; e (v) a segurança de redes de informação<sup>65</sup>. Acrescente-se a esta lista os exemplos mencionados pelo Grupo de Trabalho do art. 29<sup>66</sup>: (vi) a proteção e o exercício de direitos – como, por exemplo, direitos de expressão, de informação, de privacidade, mas também direitos patrimoniais, caso da livre iniciativa econômica, direitos de propriedade, em sentido amplo, englobando os direitos de autor e os direitos intelectuais<sup>67</sup>; (vii) publicidade e marketing de índole comercial, política ou outra; (viii) a prossecução de ações judiciais ou extrajudiciais; (ix) o monitoramento de trabalhadores, com a finalidade de segurança ou de administração empresarial; (x) a denúncia de práticas ilícitas; ou (xi) o processamento para fins históricos, científicos, estatísticos ou de investigação<sup>68</sup>.

A versatilidade e amplitude da lista apresentada (meramente exemplificativa), demonstra as dificuldades que os aplicadores do direito sentem quando confrontados com a necessidade de aplicação da hipótese do legítimo interesse.

Inclusive, durante os estudos preparatórios ao GDPR emergiu uma discussão acerca da necessidade ou não de incluir uma lista exaustiva de situações abarcadas pela hipótese do legítimo interesse. No entanto, essa solução não foi acolhida nem pelos reguladores, nem pela indústria, pois envolveria o risco de ser muito restrita e desnecessariamente prescritiva. Vale dizer que o setor empresarial desaconselhou fortemente a existência de uma lista restritiva, argumentando, principalmente, que não seria possível antecipar o curso das novas tecnologias e modelos de negócio<sup>69</sup>.

---

<sup>61</sup> Considerando 47, p. 2.

<sup>62</sup> Considerando 47, p. 6.

<sup>63</sup> Considerando 47, p. 7.

<sup>64</sup> Considerando 48.

<sup>65</sup> Considerando 49.

<sup>66</sup> GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019.

<sup>67</sup> CORDEIRO, A. Barreto Menezes. O tratamento de dados pessoais fundado em interesses legítimos. **Revista de direito e tecnologia**, Lisboa, vol. 1 (2019), no. 1, p. 1-31.

<sup>68</sup> CORDEIRO, A. Barreto Menezes. O tratamento de dados pessoais fundado em interesses legítimos. **Revista de direito e tecnologia**, Lisboa, vol. 1 (2019), no. 1, p. 1-31.

<sup>69</sup> KAMARA, Irene. DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach. **The Cambridge handbook of consumer privacy**. 2018, p. 321-352.

## 1.2 JURISPRUDÊNCIA E PRÁTICA

O presente subcapítulo abordará o desenvolvimento do legítimo interesse no seu aspecto prático: casos reais e interpretações doutrinárias. Serão analisados todos os julgados sobre a matéria no âmbito da Corte de Justiça da União Europeia, alguns casos de autoridades nacionais de proteção de dados e algumas contribuições doutrinárias sobre o assunto.

Vale dizer que os casos abordados não fornecem uma interpretação exaustiva e completa da hipótese do legítimo interesse, mas sim uma compilação fragmentada de elementos que fazem parte do desenvolvimento dessa hipótese legal e seus componentes. Ademais, muito embora todos os casos analisados tratem da interpretação do legítimo interesse no âmbito da Diretiva 95/46/CE – eis que ainda não existem casos julgados baseados no GDPR -, as ínfimas mudanças da Diretiva em relação ao Regulamento permitem que os julgados sirvam de suporte também para a interpretação do legítimo interesse no GDPR.

### 1.2.1 Casos no âmbito da Corte de Justiça da União Europeia

Muito embora a Corte de Justiça da União Europeia (CJUE) não tenha tido muitas oportunidades de interpretar a hipótese do legítimo interesse, existem alguns casos que fornecem um panorama geral de como a Corte mais alta da UE interpreta a ponderação entre os interesses, direitos e liberdades do indivíduo em relação aos interesses (legítimos ou não) dos controladores ou terceiros.

Por meio de uma pesquisa jurisprudencial na CJUE, chegou-se a apenas 6 casos em que a questão do legítimo interesse como fundamento para o tratamento de dados foi abordada, sendo a totalidade dos casos referentes ao art. 7(f) da Diretiva 95/46/CE, que perdurou de 1995 até março de 2018. Ou seja, a Corte ainda não teve a oportunidade de apreciar a incidência desse fundamento legal no âmbito do GDPR. Será possível notar, também, que muito embora a União Europeia esteja familiarizada há 24 anos com hipótese do legítimo interesse, a sua aplicação ainda carece de uniformidade e especificidade no bloco europeu.

#### 1.2.1.1 Caso Rīgas

O caso C-13/16<sup>70</sup> tratou de uma solicitação de uma empresa chamada “Rīgas”, que administrava bondes em Riga, na Letônia, que pretendia acessar, através da polícia, os dados

---

<sup>70</sup> CJUE. Case C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiks’, julgamento de 4 de Maio de 2017.

de identificação e contato de um indivíduo que estava envolvido em um acidente que resultou em um bonde danificado da empresa (mais precisamente, um passageiro abriu a porta de um táxi e arranhou o bonde).

A polícia nacional da Letônia forneceu acesso ao nome do passageiro, mas se negou a fornecer o endereço e o número telefônico, invocando restrições para divulgar informações de acordo com a lei que rege o tratamento de casos administrativos no país. A empresa de bondes contestou a decisão da polícia e ganhou em primeira instância. Com a apelação da polícia, o Tribunal de Apelação solicitou à Autoridade de Proteção de Dados da Letônia uma opinião sobre o assunto, que argumentou que a lei que rege o tratamento de casos administrativos é lei especial que se sobrepõe à lei de proteção de dados. Portanto, segundo a Autoridade, a polícia deveria aplicar as restrições da lei especial. Além disso, a autoridade salientou que mesmo que a lei de proteção de dados se aplicasse, as regras relativas aos motivos legais para processamento devem ser entendidas como uma "permissão" para processar dados pessoais, não como uma "obrigação" de processar dados pessoais.

Ou seja, mesmo que a empresa de bonde tenha um interesse legítimo como terceiro em obter os dados da polícia, a polícia não tem a obrigação de divulgar esses dados. Imposta a controvérsia, o Tribunal de Apelação decidiu suspender a instância e enviar uma questão prejudicial (*preliminary ruling*) à Corte de Justiça da União Europeia para que fosse esclarecido o que significa o tratamento ser "necessário para os interesses legítimos de terceiros" como fundamento legal para o processamento previsto no artigo 7(f) da Diretiva 95/46/CE.

A partir disso, a CJUE esclareceu que, para que um controlador se enquadre na hipótese do legítimo interesse prevista no art. 7(f) da Diretiva, três condições precisariam ser atendidas: a) a busca de um interesse legítimo pelo controlador de dados ou por terceiros, ou ainda terceiros a quem os dados são divulgados; b) a real necessidade de processar os dados pessoais para o propósito do legítimo interesse; c) por fim, que através de uma análise casuística, se pondere se as liberdades e direitos fundamentais do titular do dado estão em equilíbrio com o interesse legítimo do controlador ou terceiro:

“A este respeito, o artigo 7.o, alínea f), da Diretiva 95/46 prevê três requisitos cumulativos para que um tratamento de dados pessoais seja lícito, a saber, em primeiro lugar, a prossecução de interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, em segundo lugar, a necessidade do tratamento dos dados pessoais para a realização do interesse legítimo

e, em terceiro lugar, o requisito de os direitos e as liberdades fundamentais da pessoa a que a proteção de dados diz respeito não prevalecerem.”<sup>71</sup>

Ao fim e ao cabo, a CJUE deixou ao tribunal da Letônia a decisão sobre o caso com base nesse teste de três fases. Contudo, a Corte se posicionou no sentido de que o art. 7(f) da Diretiva 95/46 deve ser interpretado no sentido de não impor a obrigação de divulgar dados pessoais a terceiros somente para que estes terceiros intentem uma ação indenizatória perante os tribunais, mas que o art. 7(f) não se opõe a essa divulgação de dados com base em lei nacional.

Em suma, a relevância do caso para o sistema de proteção de dados na UE reside no fato de que a CJUE, a partir dessa decisão, indicou três fatores para identificar se um tratamento de dados pessoais (no caso, a divulgação de dados pessoais) pode ser fundamentado no "legítimo interesse", sendo eles: a) a existência de um interesse legítimo; b) a real necessidade do tratamento de dados ("*strict necessity*") e c) a ponderação entre os direitos e interesses em jogo.

#### 1.2.1.2 Caso Manni

No caso C-398/15<sup>72</sup>, um cidadão italiano (Sr. Manni) solicitou que a Câmara de Comércio regional apagasse seus dados pessoais do Registro Público de Empresas, depois que ele descobriu que estava perdendo clientes que verificavam seu histórico através de uma empresa privada especializada em encontrar informações no Registro Público e realizar avaliação de riscos (*rating*). Isso aconteceu porque o requerente era administrador de uma empresa que foi declarada falida há mais de 10 anos antes dos fatos no processo principal. A própria antiga empresa foi excluída do Registro Público, mas não os dados do requerente. Após a solicitação, a Câmara de Comércio rejeitou o pedido de exclusão dos dados e o recorrente contestou em sede do Tribunal local. Dada a controvérsia quanto ao dever de exclusão (ou não) dos dados do requerente, o Tribunal nacional solicitou à CJUE que esclarecesse acerca da necessidade de os Estados-membros da União Europeia manterem públicos os dados dos registros das empresas, bem como qual seria o tempo necessário para a disponibilização ao público desses dados pessoais.

---

<sup>71</sup> CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA ‘Rīgas satiks’, julgamento de 4 de Maio de 2017.

<sup>72</sup> CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, julgamento de 9 de março de 2017.

A Corte constatou, neste caso, que o tratamento de dados pessoais pela Câmara de Comércio estava legitimado por três fundamentos legais: (i) para fins de *compliance* com uma obrigação legal, (ii) para o exercício de uma autoridade oficial e efetivação de uma atividade de interesse público e, por fim, (iii) para a realização de um interesse legítimo perseguido pelo controlador ou por terceiros para os quais os dados foram divulgados.

Entre os fundamentos da Corte, em primeiro lugar constava que as pessoas em situações similares não têm o direito, *a priori*, após um certo período a partir da dissolução da empresa, de obter a exclusão dos seus dados pessoais ou o bloqueio desses dados ao público em geral. Em segundo lugar, para os propósitos do direito de se opor a esse tipo de processamento, estabeleceu que os interesses de terceiros e o comércio justo se sobrepõem aos direitos dos indivíduos que optam por participar do comércio por meio da constituição de empresas. Por fim, enfatizou também que pode haver casos individuais e específicos dessas pessoas que justifiquem a limitação do acesso do público aos seus dados pessoais, mas que tal conclusão depende de uma análise casuística.

Assim, muito embora o caso trate mais especificamente sobre a questão do direito ao esquecimento<sup>73</sup>, nota-se que a avaliação realizada pela Corte destaca a importância de detalhar as atividades de processamento de dados ao lidar com o equilíbrio entre os interesses do controlador (e, neste caso, do interesse público) e os direitos do titular em causa.

Outro ponto de vista desta sentença é que o Tribunal reconheceu a possibilidade de que uma operação de processamento de dados possa ser legitimada por três bases legais ao mesmo tempo, incluindo os “interesses legítimos”. No entanto, mesmo que isso não tenha sido explicitado, parecia que um deles estava considerando ser o principal - necessidade para a execução de uma tarefa no interesse público.

### 1.2.1.3 Caso Ryneš

No caso C-212/13<sup>74</sup>, Ryneš instalou um sistema de videovigilância fora de sua casa, monitorando sua entrada, a via pública e a entrada da casa situada em frente. O motivo do sistema de vigilância era exclusivamente proteger os bens de sua propriedade, a saúde e a vida de sua família e de si mesmo. Segundo Ryneš, tanto ele como sua família tinham sido alvo de

---

<sup>73</sup> O direito ao esquecimento consiste no direito de alguém não permitir que um fato – ainda que verdadeiro – ocorrido em determinado momento de sua vida seja exposto ao público, impedindo que lhe cause mais sofrimento ou transtorno.

<sup>74</sup> CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-212/13 Frantisek Ryneš v. Urad pro ochranu osobnich udaju, Julgamento em 11 de dezembro de 2014.

ataques (janelas quebradas, tentativas de assalto), durante vários anos, por parte de um desconhecido que não pôde ser identificado.

Na noite de 6 para 7 de outubro de 2007, houve um novo ataque: a câmara gravou imagens de um incidente em que dois suspeitos quebraram a janela de sua casa com um objeto. A filmagem foi invocada em processo criminal como meio de prova. Um dos suspeitos contestou no Tribunal a legalidade das imagens, alegando que se tratava de um tratamento ilegal de dados pessoais, pois ele não consentiu e não foi informado sobre a existência da câmara.

Dada a controvérsia, o Tribunal da Comarca de Praga solicitou esclarecimentos à CJUE antes de decidir sobre o assunto, questionando, em particular, se um sistema de videovigilância residencial instalado em uma casa familiar para proteger os bens, a saúde e a vida dos proprietários da casa pode ser qualificada como tratamento de dados pessoais "efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas", na aceção do artigo 3º, nº 2, da Diretiva 95/46.

A Corte decidiu que sistemas de vigilância por vídeo que cobrem áreas públicas não se enquadram na isenção doméstica prevista na Diretiva. No entanto, a Corte observou que, nesse caso em particular, a atividade de tratamento poderia ser conduzida com base no interesse legítimo do proprietário de casa em proteger sua propriedade, saúde e vida de sua família e de si mesmo.

#### 1.2.1.4 Caso Google Espanha

No caso C-131/12<sup>75</sup>, um cidadão espanhol pediu a um jornal que removesse um antigo artigo sobre suas dívidas pessoais. Ele também pediu ao Google que essa reportagem fosse retirada da página de resultados de pesquisas sobre seu nome. Ambas os réus rejeitaram o pedido, o que levou o requerente a apresentar uma queixa à Autoridade Espanhola de Proteção de Dados. A Autoridade decidiu que o jornal não tem a obrigação de remover o artigo (com base em exceções jornalísticas e de interesse público), mas que o Google teria a obrigação de ocultar tais resultados em seu motor de buscas quando da procura do nome do cidadão espanhol.

O Google contestou a decisão da Autoridade no Tribunal, e o Tribunal nacional decidiu instaurar um procedimento e solicitar à CJUE esclarecimentos sobre a interpretação da Diretiva 95/46/CE no que diz respeito à sua jurisdição e ao direito de exclusão de dados pessoais (direito ao esquecimento). Ao proferir a decisão, a Corte baseou-se principalmente na realização de um

---

<sup>75</sup> CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzalez, julgamento em 13 de maio de 2014.

exercício de ponderação e equilíbrio entre os direitos do titular dos dados e os interesses legítimos do Google como controlador e dos usuários da Internet como terceiros, para declarar o tratamento ilegal e permitir, portanto, o exercício do "direito ao esquecimento" do cidadão.

Nota-se que a ponderação entre (i) os interesses legítimos dos provedores de mecanismos de busca e dos usuários da Internet, de um lado, e (ii) os direitos do titular dos dados, de outro, teve um papel significativo no resultado do caso Google Espanha. Assim, a fim de verificar a existência do direito à exclusão de dados pessoais nesse caso específico (i.e., o direito ao esquecimento), a Corte analisou se o tratamento dos dados pessoais em questão era lícito ou ilícito através de uma ponderação entre tais fatores.

Ao realizar o exercício de ponderação, concluiu que os direitos do titular dos dados superam os interesses legítimos do responsável pelo tratamento e de terceiros neste caso, o que significava que o processamento não estava em conformidade com os requisitos do artigo 7º, alínea f, da Diretiva, baseado no legítimo interesse. Assim, através da ponderação, foi permitido que o direito de exclusão de dados fosse afirmado neste caso.

#### 1.2.1.5 Caso ASNEF

No casos apensos C-468/10 e C-469/10<sup>76</sup>, foi solicitado à CJUE que interpretasse o artigo 7 (f) da Diretiva 95/46 acerca do legítimo interesse do controlador no contexto da lei de transposição espanhola, que acrescentou uma condição a esse fundamento legal que restringia o possível uso de "interesses legítimos" apenas para os dados pessoais que eram disponibilizados em fontes públicas. A questão foi levada à CJUE em dois processos administrativos por duas associações profissionais distintas (uma delas dedicada à instituições financeiras e a outra ao comércio eletrônico e marketing direto), que também solicitavam esclarecimentos se o artigo 7(f) da Diretiva 46/95/CE goza de "efeito direto" (o que significa que a disposição da diretiva pode ser diretamente aplicável, em vez da lei nacional que a transpõe).

A Corte concluiu que os Estados-membros não poderiam adotar regras nacionais que transpusessem o artigo 7º, alínea f, da Diretiva 95/46 e acrescentassem condições à aplicação do legítimo interesse - como, no caso, a condição de que os dados pessoais estivessem disponíveis em fontes públicas para que o fundamento do interesse legítimo possa ser legalmente utilizado.

---

<sup>76</sup> CORTE DE JUSTIÇA DA UNIÃO EUROPEIA, Processos apensos C-468/10 e C-469/10, ASNEF and FECEMD v. Administration de Estado, julgamento em 24 de novembro de 2011.

No acórdão, a Corte ainda declarou que o artigo 7º, alínea f, possui um efeito direto de aplicação. No entanto, a Corte observou que os Estados-membros podem adotar diretrizes para o exercício de equilíbrio entre os interesses do responsável pelo tratamento ou de terceiros e os direitos e liberdades do titular dos dados, favorecendo o uso de dados pessoais disponíveis em fontes públicas para esse fim.

Em outras palavras, a decisão do caso ASNEF foi extremamente relevante para a comunidade europeia pois deixou claro que os Estados-membros não estavam autorizados a impor restrições e exigências adicionais no que diz respeito ao tratamento lícito de dados nas suas respectivas leis nacionais, especialmente em relação à hipótese prevista no art. 7(f), o legítimo interesse. Seguramente, tal impedimento imposto aos Estados-membros contribuiu para impedir a existência de discrepâncias na aplicação das legislações sobre proteção de dados entre os países membros da União Europeia, contribuindo, de certa forma, para a harmonização da legislação do bloco comunitário europeu.

#### 1.2.1.6 Caso Fashion ID

No caso C-40/17<sup>77</sup>, o mais recente dos casos abordados, a empresa Fashion ID, uma varejista alemã de roupas online, incorporou em seu próprio site o botão "curtir" disponibilizado na rede social Facebook. Contudo, o que os visitantes do referido website não sabiam é que ao clicar no botão "curtir", seus dados pessoais estavam automaticamente sendo transmitidos para o Facebook, mesmo que o sujeito não fosse membro da rede social.

Assim, a *Verbraucherzentrale NRW*, uma associação pública alemã de proteção aos direitos dos consumidores acusou a empresa Fashion ID de ter transmitido à empresa Facebook dados pessoais de visitantes de seu site, por um lado, sem o consentimento destes últimos e, por outro, em violação às obrigações de informação previstas pelas disposições relativas à proteção dos dados pessoais na Europa.

Em juízo, a associação pediu que a empresa Fashion ID pusesse fim a essa prática que considerava ilícita. Por Decisão de 9 de março de 2016, o *Landgericht Düsseldorf* (Tribunal de Düsseldorf) julgou parcialmente procedentes os pedidos da *Verbraucherzentrale NRW*, após ter reconhecido que esta tinha legitimidade para agir ao abrigo da legislação de proteção de dados alemã. A Fashion ID recorreu desta decisão para o *Oberlandesgericht Düsseldorf* (Tribunal Superior de Düsseldorf, Alemanha), e o Tribunal, em certo momento, solicitou à Corte de

---

<sup>77</sup> CORTE DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, julgado em 29 de julho de 2019.

Justiça que interpretasse inúmeras disposições da Diretiva 95/46 acerca da licitude do tratamento de dados pessoais, dentre as quais se encontrava o legítimo interesse.

Em 29 de julho de 2019, a Corte de Justiça da União Europeia concluiu, acompanhando o parecer do advogado-geral Bobek de dezembro de 2018, que muito embora o site Fashion ID e o Facebook sejam controladores conjuntos no que diz respeito às operações envolvendo a coleta e divulgação de dados pessoais por transferência ao Facebook, é necessário que cada um desses responsáveis persiga um interesse legítimo a ser considerado individualmente, na acepção do artigo 7.º, alínea f), da Diretiva 95/46, a fim de que estas sejam justificadas em relação a cada um deles.

Ou seja, segundo o posicionamento da Corte, quando o processamento de dados pessoais não requer o consentimento do usuário, mas pode ser baseado na hipótese do legítimo interesse, tanto o operador do site (no caso, Fashion ID) quanto o provedor de serviços de *plugins* (no caso, o Facebook), como controladores conjuntos, precisam buscar um interesse legítimo independente, que deve ser equilibrado com os direitos e liberdades do usuário.

Embora a Corte não tenha aplicado especificamente tal entendimento ao caso concreto, a decisão foi relevante pois responsabiliza todos os controladores conjuntos em justificarem de forma independente o tratamento de dados pessoais realizado com base na hipótese do legítimo interesse.

### 1.2.2 Casos no âmbito dos Estados-membros da União Europeia

Antes mesmo que o tema se desenvolvesse no âmbito comunitário, diversas Autoridades em Proteção de Dados dos Estados-membros da União Europeia se debruçaram sobre a questão do legítimo interesse do controlador, seja no contexto da vigência da Diretiva 95/46, que perdurou de 1995 até 2018, até a vigência do GDPR a partir de 2018. A presente seção, portanto, visa a explorar alguns destes casos decididos no âmbito das Autoridades de Proteção de Dados (também chamadas de "DPA" ou "*Data Protection Authorities*") dos Estados-membros da União Europeia.

#### 1.2.2.1 Caso Andbank - Autoridade de Proteção de Dados de Mônaco

Na deliberação 2017-068<sup>78</sup> da Autoridade de Proteção de Dados de Mônaco, um banco solicitou uma autorização à Autoridade para a utilização de um programa de monitoramento de funcionários que rastrearía os acessos aos sistemas de TI. A Autoridade considerou que a operação poderia ser legalmente fundamentada com base nos "interesses legítimos" da empresa, hipótese essa prevista na legislação nacional. O interesse legítimo da empresa, nesse caso, seria monitorar e controlar o acesso dos funcionários ao sistema e preservar a confidencialidade de informações econômicas dos clientes. Em sua deliberação, a Autoridade de Mônaco entendeu que as características do programa permitiriam o banco a processar legalmente dados pessoais dos empregados, visto que os dados seriam relevantes, adequados e não excessivos (nome, cargo, usuário e senha, identificação de conexão, data e hora do acesso e indicação da ação realizada pelo empregado). Ademais, os empregados eram informados acerca do monitoramento por meio do contrato de trabalho.

#### 1.2.2.2 Caso Whois - Autoridade de Proteção de Dados da Holanda

Em 2017, o Registro de nomes de domínio holandês<sup>79</sup> solicitou à Autoridade de Proteção de Dados da Holanda (*Autoriteit Persoonsgegevens*)<sup>80</sup> esclarecimentos sobre a licitude de publicação de dados pesquisados no Whois<sup>81</sup>.

Em atendimento à solicitação, a autoridade holandesa respondeu que essa publicação viola as leis de proteção de dados vigentes, pois nenhum dos fundamentos legais constantes na Diretiva 95/46/CE seria aplicável, incluindo a hipótese do interesse legítimo. A Autoridade considerou que o consentimento não poderia ser usado porque não seria concedido livremente; a hipótese de execução de contrato também não poderia ser utilizada, pois os detentores de

<sup>78</sup> CCIN. Délibération n° 2017-068 du 19 avril 2017 de la Commission de Contrôle des Informations Nominatives. Disponível em: <<https://www.ccin.mc/images/documents/18a57b936b7809a531f0dd12c5c57d67-Delib-2017-068-Andbank-habilitations.pdf>>. Acesso em: 10 out. 2019.

<sup>79</sup> Segundo a Autoridade holandesa, "Registries are parties who perform the technical administration of domain name extensions such as .com and .nl. Based on the rules issued by ICANN, the worldwide domain name administrator, this Dutch registry would be required to publish WHOIS-data on the internet with unlimited access". AUTORITEIT PERSOONSgegevens. Disponível em: <https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-unlimited-publication-whois-data-violates-privacy-law>. Acesso em: 30 out. 2019.

<sup>80</sup> AUTORITEIT PERSOONSgegevens. Disponível em: <<https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-unlimited-publication-whois-data-violates-privacy-law>> Acesso em: 30 out. 2019.

<sup>81</sup> Segundo o canal educativo Techtudo, "O WHOIS, cujo nome vem da expressão de língua inglesa "who is" (quem é), é um mecanismo que registra domínios, IPs e sistemas autônomos na Internet e que serve para identificar o proprietário de um site. Alimentado por companhias de hospedagem, ele reúne todas as informações pertencentes a uma página, seja ela atrelada, no Brasil, a um CNPJ ou a um CPF". ALVES, Paulo. **O que é o Whois?** Disponível em: <https://www.techtudo.com.br/noticias/noticia/2015/03/o-que-e-whois.html>. Acessado em: 30 out. 2019.

nomes de domínio não fazem parte do contrato entre a ICANN<sup>82</sup> e os Registros. Da mesma forma, o interesse legítimo não poderia ser usado porque a publicação diz respeito a todos os dados pessoais (dados excessivos) e permite acesso ilimitado a esses dados.

### 1.2.2.3 Caso Keylogger Software - Justiça Federal do Trabalho da Alemanha

No julgamento do Tribunal Federal do Trabalho alemão (*Bundesarbeitsgericht*) BAG 2 AZR 681/16 de 07 em julho de 2017<sup>83</sup>, um ex-empregado entrou com um processo judicial em face de sua ex-empregadora, alegando, entre outras coisas, que a companhia havia instalado um *software keylogger*, cuja finalidade era registrar tudo que era digitado pelos empregados nos computadores da empresa. Tendo em vista que o julgamento sobre a violação de dados pessoais foi favorável ao empregado na primeira instância, a companhia recorreu ao Tribunal Federal do Trabalho sustentando, dentre outros argumentos, o seu legítimo interesse em rastrear as atividades de seus empregados.

No julgamento da apelação, o Tribunal constatou que essa técnica de monitoramento seria demasiadamente intrusiva para ser justificada com base no legítimo interesse da companhia:

the use of a keylogger, which records all keystrokes on a business computer for covert monitoring and control of the employee is inadmissible according to § 32 (1) German Data Protection Act (BDSG) if there is no suspicion of a criminal offence or other serious breach of duty related to the employee, based on concrete facts.

Ademais, de acordo com o Tribunal, a coleta de dados através do *software keylogger* interferia radicalmente na autodeterminação informativa do titular do dado, pois o programa capturava e armazenava não só as versões finais dos trabalhos elaborados pelos usuários, mas também cada passo intermediário do método de trabalho do funcionário.

---

<sup>82</sup> Segundo a própria ICANN, "A ICANN (Corporação da Internet para Atribuição de Nomes e Números) é responsável pelo gerenciamento e pela coordenação do DNS (Sistema de Nomes de Domínio) a fim de garantir que cada endereço seja único e que todos os usuários da Internet possam encontrar todos os endereços válidos. Para isso, a ICANN supervisiona a distribuição de endereços e IP e nomes de domínio exclusivos. Ela também garante que cada nome de domínio seja associado ao endereço IP correto. A ICANN também é responsável por credenciar registradores de nomes de domínio. "Credenciar" significa identificar e definir padrões mínimos para o desempenho de funções de registro, reconhecer pessoas ou entidades que atendam a esses padrões e firmar um contrato de credenciamento que disponha as regras e os procedimentos aplicáveis à provisão de Serviços de Registrador". ICANN. **Sobre a ICANN**. Disponível em: <http://icannlac.org/PO/sobre-ICANN>. Acesso em: 30 out. 2019.

<sup>83</sup> BUNDESARBEITSGERICHT. Caso BAG 2 AZR 681/16, julgamento de 27.07.2017. Disponível em: <http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&nr=19403>. Acesso em: 30 out. 2019.

Além disso, o programa registrava e armazenava categorias especiais de dados pessoais, como senhas e nomes de usuário, informações de cartão de crédito e números PIN, sem que nenhum desses dados fossem necessários para fins de monitoramento ou vigilância. Da mesma forma, o empregado não possuía a capacidade e oportunidade de identificar se determinado conteúdo seria registrado como privado ou pessoal, de modo que não era possível optar pela restrição do acesso ao empregador<sup>84</sup>.

Ao fim e ao cabo, a Corte entendeu que havia inúmeros aspectos que tornavam o monitoramento excessivamente intrusivo aos funcionários titulares do dado pessoal, de modo que não atenderia à ponderação necessária à aplicação do legítimo interesse e que o tratamento violaria, de modo geral, a legislação europeia e alemã de proteção de dados.

#### 1.2.2.4 Caso E-commerce - Autoridade de Proteção de Dados da França

Na deliberação 2012-214<sup>85</sup>, a Autoridade Francesa de Proteção de Dados investigou uma plataforma de e-commerce em relação à sua prática de coletar e armazenar dados bancários de seus clientes por mais tempo do que o necessário para a transação. A investigação mostrou que a empresa retinha os dados bancários por padrão, no final de cada transação realizada. Dentre os dados estavam o nome do titular do cartão, número do cartão, data de validade e alguns códigos de segurança. O varejista argumentou que retinha os dados com base em dois fundamentos legais: execução de contrato e legítimo interesse do controlador. Especificamente, os interesses legítimos invocados foram a facilitação de pagamentos posteriores e a otimização das transações comerciais.

A Autoridade francesa constatou que a retenção dos dados bancários ia além da suposta finalidade de execução de um contrato para uma venda online, pois a funcionalidade de carteira eletrônica automatizada do site é para conveniência do cliente, facilitando a conclusão de vendas futuras, hipotéticas e não específicas. Do mesmo modo, a Autoridade também constatou que o processamento não poderia ser baseado no legítimo interesse do controlador, pois muito

---

<sup>84</sup> FUTURE OF PRIVACY FORUM; NIMITY PRIVACY COMPLIANCE SOFTWARE. **Processing personal data on the basis of Legitimate Interests under the GDPR**: Practical cases. Disponível em: <[https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20FPF%20-%20Legitimate%20Interests%20Report/Deciphering\\_Legitimate\\_Interests\\_Under\\_the\\_GDPR.pdf?hsCtaTracking=9cf491f2-3ced-4f9c-9ffa-5d73a77a773e%7C7469b2ec-e91c-4887-b5db-68d407654e23](https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20FPF%20-%20Legitimate%20Interests%20Report/Deciphering_Legitimate_Interests_Under_the_GDPR.pdf?hsCtaTracking=9cf491f2-3ced-4f9c-9ffa-5d73a77a773e%7C7469b2ec-e91c-4887-b5db-68d407654e23)>. Acesso em: 10 out. 2019.

<sup>85</sup> COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Deliberação 2012-214, Processada em 19 de julho de 2012. Disponível em: <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000026224040&fastReqId=770915872&fastPos=3>. Acessado em: 30 out. 2019.

embora houvesse um interesse comercial legítimo do *e-commerce* em facilitar pagamentos futuros e otimizar transações comerciais, esse interesse deveria ser equilibrado os direitos dos clientes envolvidos. A deliberação considerou que, dada a sensibilidade dos dados bancários, o direito do titular de solicitar a exclusão de seus dados após eles serem retidos por um período de tempo não poderia ser considerado uma garantia adequada aos direitos e interesses dos titulares de dados. Os dados bancários não estavam sujeitos a nenhuma eliminação final, manual ou automatizada, mas estavam sujeitos a arquivamento, dependendo de vários critérios, como o final do período de garantia. A Autoridade decidiu que a empresa teria o direito de reter os dados por no máximo 13 meses, seguindo a legislação nacional do setor financeiro (isso corresponde ao período necessário para se defender contra possíveis ações tomadas pelos bancos que tiveram que pagar clientes com base na legislação francesa). A empresa investigada também não tomou as medidas de segurança apropriadas, haja vista que os detalhes do cartão de crédito de milhões de clientes foram armazenados em texto não criptografado, em um único banco de dados, gerando o risco de que os dados se tornassem facilmente acessíveis por funcionários mal-intencionados ou invasões externas.

Resumidamente, o caso analisado nos mostra que muito embora a empresa tivesse um legítimo interesse para processar os dados pessoais, ela falhou em adotar medidas suficientes de segurança visando a resguardar os dados de seus clientes. Assim, restou prejudicado o teste de ponderação entre os direitos e liberdades do titular e o interesse legítimo do controlador.

### 1.2.3 O teste de ponderação/proportionalidade

O legítimo interesse do controlador vem sendo há anos um dos principais fundamentos que justificam o tratamento de dados em empresas europeias, e mesmo assim ainda carece de delimitações e parâmetros bem estabelecidos de aplicação. Trata-se de uma redação flexível que deixa uma grande margem de interpretação e que muitas vezes já conduziu - como a experiência europeia demonstra - à complexidade e à falta de previsibilidade e segurança jurídica no tratamento de dados pessoais<sup>86</sup>. No entanto, se for utilizado no contexto correto e

---

<sup>86</sup> Segundo o parecer 06/2014 grupo de trabalho instituído pelo art. 29 da Diretiva 95/46/CE, "Os estudos realizados pela Comissão no âmbito da revisão da Diretiva, bem como a cooperação e o intercâmbio de opiniões entre as autoridades nacionais responsáveis pela proteção de dados (a seguir designadas por «ARPD»), revelaram a falta de harmonização na interpretação do artigo 7.º, alínea f), da diretiva, que conduziu a aplicações divergentes nos Estados-Membros.". GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE.** Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019.

com a aplicação de critérios adequados, a hipótese de tratamento sob o fundamento do legítimo interesse possui um papel essencial a desempenhar, principalmente por permitir que a lei não engesse novas práticas mercadológicas e os inevitáveis avanços tecnológicos.

Tendo em vista as incertezas e imprecisões que circundam o conceito do tratamento legal de dados pessoais com base no legítimo interesse do controlador, com a finalidade de esclarecer os parâmetros de aplicação dessa hipótese, em 2014 o Grupo de Trabalho instituído pelo artigo 29 da Diretiva 95/46/CE<sup>87</sup> apresentou um parecer consultivo especificamente sobre a matéria. O parecer sugere que o tratamento de dados com base na hipótese do legítimo interesse está subordinado a um teste de ponderação e proporcionalidade - o *legitimate interest assessment* (LIA) - que pondera os interesses legítimos do responsável pelo tratamento - ou terceiro a quem os dados sejam comunicados - em relação aos interesses e direitos fundamentais do titular em causa.

Em linhas gerais, o documento prevê um teste multifatorial composto por quatro passos sequenciais: a) a avaliação do legítimo interesse do responsável pelo tratamento; b) avaliação do impacto sobre o titular do dado pessoal; c) o equilíbrio entre os fatores "a" e "b"; e d) as salvaguardas tomadas pelos responsáveis pelo tratamento dos dados pessoais para prevenir consequências negativas aos titulares dos dados<sup>88</sup>.

No âmbito da avaliação do primeiro fator ("a", existência de um interesse legítimo), o Grupo de Trabalho se dedica a explorar o conceito de interesse legítimo. Muito embora o Parecer adiante que é impossível fazer juízos de valor relativamente a todos os eventuais interesses legítimos, é possível fornecer algumas orientações. Segundo o parecer, o interesse poderá ser legítimo se (i) possibilitar o exercício de um direito fundamental<sup>89</sup>- ou, em outras

---

<sup>87</sup> O artigo 29 da Diretiva 95/46/CE criou um grupo independente e de natureza consultiva com a finalidade de (i) orientar os estados-membros e garantir a aplicação uniforme da Diretiva, (ii) emitir pareceres à Comissão sobre o nível de proteção na comunidade europeia, (iii) aconselhar a Comissão sobre projetos de alteração da diretiva ou atividades relacionadas à proteção de dados pessoais e (iv) emitir pareceres sobre os códigos de conduta elaborados a nível comunitário.

<sup>88</sup> Vale ressaltar que existem variações deste teste, que ora é composto por quatro passos, ora é composto por três passos. A título ilustrativo, a Information Commissioner Office (ICO) do Reino Unido resume o teste em apenas três fatores: a existência de um legítimo interesse, a real necessidade do tratamento de dados para a finalidade do tratamento e, por fim, a ponderação entre o legítimo interesse do controlador e os interesses/direitos do titular (UK INFORMATION COMMISSIONER OFFICE. **Guide to the general data protection regulation** (GDPR). Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>. Acesso em: 11 out. 2019.

<sup>89</sup> Entre os direitos e as liberdades fundamentais, o Parecer destaca os consagrados na Carta dos Direitos Fundamentais da União Europeia ("Carta") e na Convenção Europeia dos Direitos do Homem ("CEDH"): direito à liberdade de expressão e informação, a liberdade das artes e das ciências, o direito de acesso aos documentos, o direito à liberdade e à segurança, a liberdade de pensamento, de consciência e religião, a liberdade de empresa, o direito de propriedade, o direito à ação e a um tribunal imparcial ou a presunção de inocência e os direitos de

palavras, não obstar o exercício de um direito fundamental pelo titular<sup>90</sup>; (ii) corresponder total ou parcialmente a um interesse público ou interesse da comunidade em geral<sup>91</sup>; (iii) se identificar com outros fundamentos de licitude elencados no artigo 6º do GDPR; ou (iv) for merecedor de reconhecimento jurídico, cultural/social da legitimidade dos interesses<sup>92</sup>. De forma mais objetiva, o Grupo de Trabalho estabelece que para ser considerado legítimo, um interesse deve ser, cumulativamente, lícito (respeitar o direito da UE e o direito nacional), suficientemente claro e concreto e representar um interesse real e atual (não especulativo).

Ainda, segundo A. Barreto Menezes Cordeiro, por mais que inexista uma definição concreta de interesse legítimo, resta-nos reconhecer, à luz dos dados disponíveis em cada situação, que o conceito de interesse legítimo abrange todas as vantagens, legais ou fáticas, próprias ou alheias, cuja prossecução em concreto seja lícita, atendendo ao GDPR e ao Direito vigente. Após verificar a existência de interesses concretos, caberia ao intérprete-aplicador analisar se desse mesmo tratamento resulta uma afetação "dos interesses ou direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais"<sup>93</sup>.

---

defesa. GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 53.

<sup>90</sup> Segundo o parecer, "Para que o interesse legítimo do responsável pelo tratamento prevaleça, o tratamento de dados deve ser «necessário» e «proporcionado», de forma a possibilitar o exercício do direito fundamental em causa". GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 53

<sup>91</sup> Segundo o parecer, "Quanto mais preponderante for o interesse público ou o interesse da comunidade em geral, e quanto mais o facto de o responsável pelo tratamento poder atuar e tratar os dados na prossecução desse interesse for claramente reconhecido e esperado pela comunidade e pelas pessoas em causa, mais valor esse interesse legítimo tem na ponderação". GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 55.

<sup>92</sup> Como exemplos desse reconhecimento, o Parecer traz os seguintes casos: (i) quando há conformidade com a legislação do Estado-membro ou das orientações da Autoridade de Proteção de Dados respectiva; (ii) quando existem quaisquer orientações validamente adotadas e não vinculativas emitidas pelos organismos competentes, como, por exemplo, por autoridades reguladoras, que incentivem os responsáveis pelo tratamento a tratar os dados na prossecução do interesse em causa; e (iii) quando o tratamento atende as expectativas culturais e sociais, mesmo que sem base jurídica específica. GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 56.

<sup>93</sup> CORDEIRO, A. Barreto Menezes. O tratamento de dados pessoais fundado em interesses legítimos. **Revista de direito e tecnologia**, Lisboa, vol. 1 (2019), no. 1, p. 1-31.

Já o segundo fator ("b", o impacto sobre o titular do dado pessoal) engloba todas as questões relacionados com o tratamento e com os dados pessoais *per se*: (i) a avaliação do impacto do tratamento<sup>94</sup> – positivo, negativo, objetivo ou subjetivo<sup>95</sup>; (ii) a natureza dos dados<sup>96</sup>; (iii) a forma como os dados são tratados<sup>97</sup>; (iv) as expectativas razoáveis da pessoa em causa; e (v) o *status* ou poder econômico do responsável pelo tratamento dos dados e o *status* da pessoa em causa<sup>98</sup>, nomeadamente a existência de uma relação de proximidade ou de desigualdade entre as partes.

No terceiro fator ("c", o equilíbrio entre os fatores "a" e "b"), o Grupo de Trabalho sugere a realização de um exercício de ponderação entre os interesses e direitos em jogo. Nesse sentido, é necessário que o tratamento seja realizado em atenção à proporcionalidade e transparência,

---

<sup>94</sup> Neste fator, existem dois elementos-chave: por um lado, a probabilidade do risco concretizar-se, e, por outro lado, a gravidade das consequências que o risco ocasionaria. GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 60.

<sup>95</sup> No que toca à avaliação de impacto do tratamento de dados, deve-se ter em conta as potenciais ações e decisões futuras por parte de terceiros, situações nas quais o tratamento de dados poderá conduzir à discriminação e difamação da pessoa em causa, ou, de forma mais abrangente, situações nas quais exista o risco de prejudicar a reputação, o poder de negociação e a autonomia do titular do dado. Esses seriam os impactos objetivos negativos. Já os subjetivos, seriam os impactos emocionais que podem acometer os titulares em causa, tais como irritação, medo ou angústia que podem ser provocados pelo fato do titular perder o controle sobre o destino dos seus dados pessoais, que podem estar sendo utilizados de maneira indevida e abusiva. GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 58.

<sup>96</sup> Neste fator é relevante se verificar se o tratamento envolve dados sensíveis dos titulares (como dados biométricos, dados genéticos, dados de comunicações, dados de localização e outros tipos de informações que exijam proteção especial). GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 60.

<sup>97</sup> Segundo o parecer: "Dados aparentemente inócuos, quando sejam tratados em grande escala e combinados com outros dados, podem dar azo a inferências sobre dados mais sensíveis" e "Em geral, quanto mais negativo ou incerto for o impacto do tratamento, mais improvável é que o tratamento venha a ser considerado, em termos gerais, legítimo". GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 62.

<sup>98</sup> No caso da pessoa natural, por exemplo, será relevante se verificar se de algum modo a pessoa pertence a um segmento mais vulnerável da sociedade que requeira um tratamento especial, como, por exemplo, as crianças e os idosos. GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 64

garantindo-se que o impacto nas pessoas seja reduzido, que seja menos provável que os interesses ou os direitos e liberdades fundamentais das pessoas em causa sejam afetados e que, por isso, seja mais provável que o responsável pelo tratamento de dados possa invocar o legítimo interesse<sup>99</sup>.

No quarto fator ("d", as salvaguardas tomadas pelos sujeitos que processam os dados pessoais para prevenir consequências negativas ao titular dos dados), o Grupo de Trabalho elenca inúmeras "garantias" que visam a melhor tutelar os interesses dos titulares dos dados. A título ilustrativo, o documento refere: (i) medidas técnicas e organizativas para assegurar que os dados não possam ser utilizados para tomar decisões ou outras medidas em relação às pessoas; (ii) utilização ampla de técnicas de anonimização; (iii) agregação de dados; (iv) tecnologias para reforçar a proteção da privacidade, privacidade desde a concessão, avaliação de impacto na privacidade e na proteção de dados; (v) maior transparência; (vi) direito generalizado e incondicional de optar por não permitir o tratamento; e (vii) portabilidade dos dados e medidas afins para capacitar as pessoas em causa<sup>100</sup>.

Nota-se, portanto, que o Grupo de Trabalho ao elaborar o teste de ponderação visou a adoção de uma abordagem equilibrada, que assegura aos responsáveis pelo tratamento de dados a flexibilidade necessária em situações que não se verifique um impacto negativo e indevido nos titulares dos dados, proporcionando, ao mesmo tempo, uma certa segurança jurídica e garantia de que a disposição aberta do legítimo interesse não será utilizada de forma abusiva pelos controladores. Nota-se, ao mesmo tempo, que os dois principais componentes do interesse legítimo são conceitos jurídicos indeterminados (legítimo interesse do controlador e legítima expectativa do titular), o que torna a análise ainda mais complexa<sup>101</sup>.

A fim de elucidar as referências contidas no presente capítulo, a tabela elaborada abaixo resume o passo-a-passo do teste de ponderação sugerido pelo Grupo de Trabalho do artigo 29, simulando cada etapa necessária para aferição do enquadramento de um tratamento de dados na hipótese do legítimo interesse do controlador:

---

<sup>99</sup> GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 64.

<sup>100</sup> GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019. p. 66.

<sup>101</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro:Forense, 2019. p. 252.

Quadro 1 – Passo-a-passo do “teste de ponderação” sugerido pelo GT29

<b>PASSO 1</b>	Verificar qual das hipóteses de tratamento a operação se enquadra. Se aparentemente for enquadrada com base no interesse legítimo, proceder ao passo 2.
<b>PASSO 2</b>	Qualificar o interesse como legítimo ou ilegítimo. Para ser considerado legítimo, o interesse deve preencher cumulativamente as seguintes condições: (i) ser lícito; (ii) ser suficientemente claro e concreto, permitindo que o teste de ponderação seja feito em função dos interesses e direitos fundamentais do titular do dado; (iii) representar um interesse real e presente/atual (não especulativo).
<b>PASSO 3</b>	Determinar se o tratamento é realmente necessário para atingir o interesse pretendido. Neste passo, deve-se averiguar se existe algum outro meio menos invasivo para atingir a finalidade pretendida e servir o interesse legítimo do responsável pelo tratamento do dado.
<b>PASSO 4</b>	Avaliar se o interesse do responsável pelo tratamento de dados está sendo sobreposto aos direitos ou interesses fundamentais dos titulares dos dados. Alguns parâmetros a serem seguidos são: (i) considerar a natureza dos interesses do controlador (se é um direito fundamental, interesse público, etc); (ii) Levar em conta a natureza dos dados (especialmente se for dado sensível); (iii) Considerar o <i>status</i> do titular dos dados (menor de idade, funcionário, idoso, etc) e do controlador (por exemplo, se uma organização comercial está em uma posição dominante no mercado); (iv) Levar em conta a forma como os dados são processados (grande escala, mineração de dados, <i>profiling</i> , divulgação para um grande número de pessoas ou publicação); (v) Identificar os direitos fundamentais e/ou interesses do titular dos dados que podem ser afetados; (vi) Considerar as expectativas razoáveis dos titulares de dados; (vii) Avaliar os impactos no titular dos dados e comparar com o benefício esperado do processamento.
<b>PASSO 5</b>	Identificar e implementar salvaguardas adicionais apropriadas, resultantes do <i>duty of care and diligence</i> , tais como: (i) minimização de dados (limitações rigorosas na coleta de dados ou exclusão imediata de dados após o uso); (ii) medidas técnicas e organizacionais para garantir que os dados não possam ser utilizados para tomar decisões ou outras ações em relação a indivíduos ("separação funcional"); (iii) uso de técnicas de anonimização, agregação de dados, tecnologias de melhoria de privacidade, <i>privacy by design</i> , avaliações de impacto de privacidade e proteção de dados; (iv) aumento da transparência, direito geral e incondicional de “contestar” ( <i>opt-out</i> ), portabilidade de dados e quaisquer outras medidas que possam empoderar o titular do dado.
<b>PASSO 6</b>	Demonstrar <i>compliance</i> e garantir transparência. Isso deverá ser feito através: (i) da elaboração de documentação de um “plano” dos passos de 1 a 5 para justificar o tratamento antes de este ter início; (ii) da informação aos titulares dos dados sobre as razões pelas quais acredita que a ponderação está a favor do responsável pelo tratamento; (iii) da manutenção da documentação disponível para as autoridades de proteção de dados pertinentes.
<b>PASSO 7</b>	Em caso de oposição do titular do dado, garantir que existem mecanismos adequados e de fácil utilização que permitam reavaliar o equilíbrio no que diz respeito à pessoa em causa e pôr fim ao tratamento dos dados se a reavaliação revelar que os interesses e direitos do titular prevaleceram.

Fonte: O autor (2019)

## 2 O LEGÍTIMO INTERESSE DO CONTROLADOR COMO FUNDAMENTO PARA O TRATAMENTO DE DADOS PESSOAIS NO BRASIL

### 2.1 MARCO LEGAL: A LGPD

A hipótese de tratamento de dados pessoais com base no legítimo interesse do controlador existe no Brasil desde 2018, com a aprovação da Lei Geral de Proteção de Dados (Lei 13.709 de 2018, LGPD). Como se verá a seguir, tão forte é a influência europeia em nossa lei de proteção de dados que o legislador brasileiro praticamente importou, com algumas pequenas alterações, a quase integralidade do dispositivo acerca do legítimo interesse previsto no GDPR europeu. Apesar de tais similitudes, o presente capítulo visa a explorar a conceitualização e desenvolvimento do legítimo interesse exclusivamente no contexto brasileiro.

A LGPD, em seu artigo 7º, assim inaugura a previsão da hipótese do legítimo interesse em nosso ordenamento<sup>102</sup>:

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;

A fim de complementar a redação do artigo 7º, IX, o legislador forneceu algumas delimitações complementares em sede do artigo 10 da Lei:

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

I - apoio e promoção de atividades do controlador; e

---

<sup>102</sup> Nota-se, aqui, a grande semelhança com a redação do art. 6º, alínea "f", do GDPR: "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: (...) 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". UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 04/05/2016. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 20 set. 2019.

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 baseado 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.

Percebe-se que o legislador brasileiro optou - intencionalmente - por não trazer um conceito específico de interesse legítimo, limitando-se a indicar duas situações exemplificativas e genéricas em que este fundamento pode ser identificado: quando houver (i) apoio e promoção de atividades do controlador; e (ii) proteção, em relação ao titular, do exercício regular de direitos ou prestação de serviços que o beneficiem, respeitadas as suas legítimas expectativas e os direitos e liberdades fundamentais<sup>103</sup>.

À primeira vista, uma miríade de situações poderia se encaixar nas descrições contidas nos incisos I e II do artigo 10º, e, por conta disso, o legislador trouxe alguns limites nos parágrafos subsequentes. Assim, os seguintes limites resultam da interpretação do artigo 10º da LGPD: em primeiro lugar, que o interesse legítimo do controlador no tratamento de dados não se admite em vista de critérios genéricos, senão em acordo com o exame de situações concretas; em segundo lugar, que abrange somente os dados pessoais estritamente necessários para a finalidade pretendida (art. 10, §1º, LGPD); em terceiro lugar, que devem ser respeitadas, em qualquer caso, as legítimas expectativas do titular dos dados (art. 10, II, LGPD), o que se deve considerar tendo em vista tanto da informação efetivamente prestada no caso de ter havido consentimento, ou ainda a proteção de sua privacidade, considerada nos termos em que acredita, de modo legítimo, resguardar certas informações sobre si do conhecimento de terceiros. Além destas situações, merece ser destacada a exigência de adotar medidas de transparência no uso dos dados sob a justificativa do legítimo interesse do controlador (art. 10, § 2º), de modo a permitir, inclusive, que o titular dos dados se oponha a esta utilização, sem prejuízo da mitigação dos riscos que deve perseguir<sup>104</sup>.

---

<sup>103</sup> MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. LGPD: Lei Geral de Proteção de Dados comentada. Viviane Nóbrega Maldonado, Renato Opice Blum, coordenadores. São Paulo: **Revista dos Tribunais**. 2019, p. 194.

<sup>104</sup> MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**. vol. 1009/2019. 2019. p. 9.

Quanto ao aspecto do desenvolvimento histórico do legítimo interesse no cenário brasileiro, vale ressaltar que o caráter aberto dessa previsão legal não foi por acaso, pois surgiu como consequência de um apelo derivado do setor empresarial<sup>105</sup>. Tanto isso é verdade que na primeira versão do anteprojeto da Lei Geral de Proteção de Dados, o legítimo interesse sequer constava no rol de hipóteses de legais para o tratamento de dados pessoais<sup>106</sup>, tendo gerado inúmeros debates entre o setor empresarial e a sociedade civil sobre sua efetividade e real necessidade de ser transposto ao ordenamento brasileiro.

De um lado, uma camada do setor empresarial<sup>107</sup> sustentou ser necessário transpor a hipótese do legítimo interesse do sistema europeu para a futura lei brasileira, por conta, justamente, da flexibilidade proporcionada pelo legítimo interesse, que seria apropriada ao cenário atual de uso intensivo de dados pessoais no mercado e dispensaria a necessidade de recorrer a todo momento ao consentimento do titular, o que seria economicamente inviável para os controladores. Por outro lado, a comunidade civil e a academia<sup>108</sup> puxaram um cabo de força para que a inclusão do legítimo interesse apenas viesse acompanhada de requisitos específicos para sua aplicação. O principal argumento era que a futura lei brasileira não repetisse o equívoco da Diretiva 95/46/CE da União Europeia (falta de orientações e uniformidade na aplicação), de modo que fossem asseguradas a previsibilidade e segurança jurídica na interpretação desta hipótese legal no Brasil<sup>109</sup>.

Tal debate traz à tona duas perspectivas: se, por um lado, a flexibilidade é bem-vinda pelo setor empresarial como modo de incentivar a inovação, por outro, ela remove um certo

---

<sup>105</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 250.

<sup>106</sup> Note-se que o legítimo interesse não constava no artigo 9º do anteprojeto. Disponível em: <<http://culturadigital.br/dadospessoais/files/2010/11/PL-protecao-de-dados.pdf>>. Acesso em: 12 out. 2019.

<sup>107</sup> Segundo o mapeamento realizado pela InternetLab, verificaram-se os seguintes atores nos debates públicos pelo setor empresarial: ITI, Centre for Information Policy Leadership, GSMA, Fiesp, Iab, Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações, Associação Brasileira da Indústria Elétrica e Eletrônica, Associação Brasileira de Internet, BSA The Software Alliance, Sky, US Business Council e CNeg, Febraban, RELX Group, Cisco, Brasscom, Camara BR, Claro e VIVO. INTERNET LAB. São Paulo: InternetLab Pesquisa em Direito e Tecnologia. **InternetLab Reporta nº 17 – Debate Público de Proteção de Dados Pessoais**. Disponível em: <<https://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-no-17-debate-publico-de-protecao-de-dados-pessoais/>>. Acesso em: 09 out. 2019.

<sup>108</sup> Segundo o mapeamento realizado pela InternetLab, verificaram-se os seguintes atores nos debates públicos pela academia e sociedade civil: Grupo de Políticas Públicas para o Acesso à Informação da Universidade de São Paulo e Instituto de Tecnologia e Sociedade do Rio de Janeiro. INTERNET LAB. São Paulo: InternetLab Pesquisa em Direito e Tecnologia. **InternetLab Reporta nº 17 – Debate Público de Proteção de Dados Pessoais**. Disponível em: <<https://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-no-17-debate-publico-de-protecao-de-dados-pessoais/>>. Acesso em: 09 out. 2019.

<sup>109</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 251.

grau de segurança jurídica e pode criar brechas no sistema jurídico. Este é o caso quando as normas são formuladas de forma ambígua e nenhuma orientação é fornecida. Portanto, o próximo subcapítulo do trabalho se dedica a estabelecer alguns limites à aplicação do legítimo interesse no Brasil.

## 2.2 SUBSÍDIOS À APLICAÇÃO DO LEGÍTIMO INTERESSE NO BRASIL

Ao enfatizar que deve haver os registros de tratamento de dados pessoais com base no legítimo interesse do controlador<sup>110</sup> ao lado de um conjunto de obrigações para quem queira se valer de tal base legal<sup>111</sup>, a Lei Geral de Proteção de Dados brasileira aponta para a *necessidade* de execução de um teste de proporcionalidade<sup>112</sup>.

Além disso, a similaridade das disposições acerca do legítimo interesse na LGPD e no GDPR apontam para uma convergência quanto à interpretação e aplicação do legítimo interesse no Brasil. Nesse sentido, de modo sistemático, pode-se observar que a legislação brasileira estabelece os seguintes limites para a utilização da hipótese do legítimo interesse como fundamento para o tratamento de dados pessoais: a) a verificação da legitimidade do interesse (art. 10, caput e I, da LGPD<sup>113</sup>); b) a verificação da necessidade do tratamento de dados (art. 10, §1º, da LGPD<sup>114</sup>); c) o balanceamento dos impactos ao titular dos dados e suas legítimas

---

<sup>110</sup> LGPD, 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". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>111</sup> LGPD, art. 10: "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades 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 baseado 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". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>112</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 253.

<sup>113</sup> "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>114</sup> "§1º. Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados". BRASIL. **Lei nº 13.709, de 14 de**

expectativas (art. 7, IX<sup>115</sup> e 10, II, da LGPD<sup>116</sup>); e, por fim, d) as salvaguardas necessárias para garantir a transparência e documentação do tratamento de dados com base no legítimo interesse (art. 10, §§ 2 e 3, LGPD<sup>117</sup>).

Agora, se passará a analisar particularmente cada um desses requisitos articulados pela LGPD. Em relação ao primeiro requisito (legitimidade do interesse), é necessário se verificar a.1) se o tratamento de dados não contraria outros comandos legais, como leis esparsas e legislação infralegal<sup>118</sup> e a.2) se o interesse do controlador está claramente articulado<sup>119</sup>, de modo que esteja previsto em uma situação em concreto que lhe dê suporte. Quanto mais articulada e concreta for a legitimidade do interesse, a situação e a finalidade para a qual os dados pessoais serão tratados pelo controlador, mais fácil será analisar a aplicabilidade do legítimo interesse nos passos subsequentes.

Sobre o segundo requisito estabelecido pela LGPD (dados pessoais "estritamente necessários"), uma vez bem articulado e definido o interesse do controlador, será necessário se verificar se: b.1) os dados coletados são aqueles estritamente necessários para garantir a finalidade pretendida pelo controlador, ou seja, se haveria algum outro meio menos intrusivo de atingir a mesma finalidade/resultado por meio de uma quantidade menor de dados e b.2) se

---

**agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>115</sup> "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) 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". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>116</sup> "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: (...) 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". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>117</sup> "§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado 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". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>118</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019. p. 253.

<sup>119</sup> ZANFIR-FORTUNA, Gabriela et al. Processing personal data on the basis of legitimate interests under the GDPR: practical cases. **Future of Privacy Forum**, 2018. p. 5.

o tratamento de dados poderia ter como base outros fundamentos legais previstos no art. 7º da LGPD<sup>120</sup>, como o consentimento, execução de contrato, tutela da saúde, etc.

A terceira e principal etapa do teste de proporcionalidade proposto pela LGPD trata-se, finalmente, da sobreposição entre os direitos e liberdades do titular de dados, e os interesses legítimos do controlador. Nessa fase, deve-se investigar: c.1) se o uso do dado que será fundamentado na hipótese do legítimo interesse corresponde às legítimas expectativas do titular dos dados. Segundo Bruno Bioni, esse uso é parametrizado pela noção de compatibilidade entre o uso adicional (novo) e aquele que originou a coleta dos dados pessoais<sup>121</sup>. Além disso, deve-se verificar c.2) se o uso secundário dos dados seria legitimamente esperado pelo titular dos dados<sup>122</sup>, de modo que o tratamento pelo legítimo interesse não poderia surpreendê-lo; e c.3) de que forma os titulares dos dados são impactados, especialmente repercussões negativas em termos de discriminação e autonomia informativa, de modo a atentar suas liberdades e direitos fundamentais. Em síntese, nessa etapa da verificação da aplicação do legítimo interesse, é necessário se avaliar se o fluxo informacional é apropriado e íntegro para o livre desenvolvimento da personalidade e liberdade do titular<sup>123</sup>.

Por fim, a quarta e última etapa articulada pela LGPD é a garantia de salvaguardas aos titulares dos dados. Dentro desse conceito, reforça-se d.1) o dever de transparência; d.2) o poder de tomada de decisões pelo titular, para se opor ao tratamento de dados que considerar incompatível com suas legítimas expectativas (*opt-out*) e, por fim, o controlador deve adotar d.3) ações que mitiguem os riscos ao titular, através de salvaguardas como anonimização de dados, sendo esse o sentido da previsão de eventual necessidade de elaboração de um relatório de impacto à privacidade na LGPD<sup>124</sup>.

---

<sup>120</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 254.

<sup>121</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 254.

<sup>122</sup> Sobre as legítimas expectativas do titular com base no Parecer 06/2014, "the second factor focuses on the specific context in which the data were collected and the reasonable expectations of the data subjects as to their further use based on that context. In other words, the issue here is what a reasonable person in the data subject's situations would expect his or her data to be used for based on the context of the collection". GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019, p. 24.

<sup>123</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 255.

<sup>124</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 255.

Assim como foi realizado no capítulo anterior sobre o teste de proporcionalidade da legislação europeia, a fim de resumir os passos abordados no presente capítulo, ilustrou-se na tabela abaixo os quatro passos/limites estabelecidos pela LGPD para a aplicação e interpretação do legítimo interesse do controlador:

Quadro 2 - O Legítimo Interesse na LGPD

<b>Passo</b>	<b>Descrição</b>	<b>Fundamento legal</b>
Passo 1	<b>Verificação da legitimidade do interesse do controlador:</b> o interesse do controlador deverá ser lícito e concreto.	"O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para <b>finalidades legítimas</b> , consideradas a partir de situações <b>concretas</b> " - art. 10, caput, LGPD.
Passo 2	<b>Verificação da necessidade:</b> somente os dados pessoais estritamente necessários poderão ser fundamentados no legítimo interesse.	"Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados <b>pessoais estritamente necessários</b> para a finalidade pretendida poderão ser tratados" - art. 10, §1, LGPD.
Passo 3	<b>Balanceamento</b> entre interesse do controlador e os direitos, liberdades fundamentais e expectativas do titular.	"Proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, <b>respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais</b> , nos termos desta Lei" - art. 10, II, LGPD.  "Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de <b>prevalecerem direitos e liberdades fundamentais do titular</b> que exijam a proteção dos dados pessoais" - art. 7, IX, LGPD.
Passo 4	<b>Garantia de salvaguardas</b> para garantir transparência e documentação no tratamento de dados.	"O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse." - art. 10, §2, 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" - art. 10, §3, LGPD.

Fonte: O autor (2019)

Por fim, nota-se, também, que a nossa Lei Geral de Proteção de Dados traz, em seu art. 10, §3<sup>125</sup>, a necessidade de atuação da Autoridade Nacional de Proteção de Dados no controle da aplicação da hipótese do legítimo interesse.

<sup>125</sup> "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".

## CONSIDERAÇÕES FINAIS

A principal dificuldade de aplicação da hipótese do legítimo interesse para o tratamento lícito de dados é, com certeza, a vagueza do termo "legítimo interesse". A falta de orientações claras sobre a aplicação desta hipótese legal gera desconfiança e receio na sua aplicação. No entanto, muito embora a hipótese do legítimo interesse possua uma natureza imprecisa e suscite questões complexas quanto ao seu alcance, tal não significa que essa opção deva ser considerada como último recurso quando as outras bases legais não são aplicáveis. De igual modo, também não deve ser considerada uma opção preferencial ou de aplicação demasiadamente flexível<sup>126</sup>, tal como uma "carta coringa" dos controladores. Pelo contrário: a hipótese do legítimo interesse pode - e deve - ter sua própria autonomia e relevância, desde que determinado o seu alcance.

O presente estudo, ao tratar do desenvolvimento da hipótese legal do legítimo interesse no cenário europeu e brasileiro, traçou um caminho que desvendou os critérios e limites hoje existentes para a aplicação dessa hipótese legal e nos permitiu realizar uma análise crítica e chegar a algumas conclusões.

Em primeiro lugar, claro está que, tanto na LGPD, quanto no GDPR, a aplicação da hipótese do legítimo interesse aponta para a *necessidade* da execução de um teste de proporcionalidade. Essa necessidade de se ponderar cada situação concreta se dá principalmente por dois motivos: (i) porque dois dos principais componentes dessa difícil equação são conceitos jurídicos indeterminados ("legítimo interesse do controlador" e "legítima expectativa do titular") e (ii) a própria lei (LGPD e GDPR) determina um conjunto de obrigações para quem queira se valer dessa base legal, inclusive a ponderações entre direitos e liberdades do titular do dado em relação ao interesse legítimo do controlador.

Como foi visto ao longo da primeira parte do trabalho, na União Europeia o Grupo de Trabalho do art. 29 já sistematizou um teste multifatorial para identificar se o tratamento poderá ser baseado no fundamento legal do legítimo interesse. Da mesma forma, conforme foi abordado na segunda parte do trabalho, a LGPD também aponta para a necessidade de realizar

---

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

<sup>126</sup> GRUPO DE TRABALHO DO ARTIGO 29. **Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento de dados na aceção do artigo 7º da Diretiva 95/46/CE**. Adotado em 9 de abril de 2014. Disponível em: [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Acesso em: 11 out. 2019.

um teste similar, dada a equivalência entre a legislação europeia e brasileira neste ponto específico. Vale elucidar que o presente trabalho não sugere a aplicação direta, no Brasil, do teste elaborado pela experiência europeia. O que se pretende, contudo, é identificar os pontos de convergência entre ambas as legislações e avaliar de que modo a experiência europeia pode servir de inspiração para a aplicação dessa cláusula aberta no Brasil, tendo em vista a entrada em vigor da LGPD em agosto de 2020.

Em resumo, ambas as leis sugerem que a proporcionalidade seja avaliada a partir dos seguintes parâmetros: (i) a legitimidade do interesse – ou seja, se o interesse almejado pelo controlador é lícito, concreto e não especulativo; (ii) a necessidade do tratamento - nesse passo, deve-se averiguar se existe algum outro meio menos invasivo para atingir a finalidade pretendida e servir o interesse legítimo do responsável pelo tratamento do dados, pois o dado para ser tratado com base no legítimo interesse deve ser estritamente necessário; (iii) o balanceamento entre direitos e liberdades - em que seria necessário se avaliar se o interesse do responsável pelo tratamento de dados está sendo sobreposto aos direitos ou interesses fundamentais dos titulares dos dados, bem como suas legítimas expectativas, e (iv) a adoção das salvaguardas necessárias para garantir a transparência e documentação das operações que se utilizam do legítimo interesse como base legal para tratamento.

Em segundo lugar, conclui-se que, no Brasil, a árdua tarefa de determinar novos parâmetros que delimitem o legítimo interesse do controlador será atribuída especialmente à Autoridade Nacional de Proteção de Dados<sup>127</sup> que, juntamente aos impactos técnicos do tratamento, deverá definir e desenvolver soluções ágeis e seguras para a delimitação dessa cláusula. Caso assim não seja, as soluções serão centralizadas em conflitos judiciais, acarretando não apenas morosidade na proteção de dados, como também a redução do próprio papel da Autoridade Nacional e da aplicação do artigo 10, §3º, da LGPD<sup>128</sup>.

Em terceiro lugar, ficou claro que a aplicação de um teste de ponderação/proporcionalidade ainda está longe de ser um processo simples<sup>129</sup>, pois cada situação deve ser ponderada de acordo com suas próprias particularidades. Um indício é que muito embora na União Europeia a hipótese do legítimo interesse venha sendo tratada há anos pelos tribunais, em poucos casos houve a oportunidade de aplicação direta do teste de

---

<sup>127</sup> FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. São Paulo: **Revista dos Tribunais**, 2019. p. 475.

<sup>128</sup>"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".

<sup>129</sup>FERRETTI, Federico. Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? **Common Law Market Review** 51, 2014, p. 843-868.

ponderação elaborado pelo Grupo de Trabalho 29. Ainda, mesmo que os Considerandos 47 e 49 do GDPR tragam consigo uma série de exemplos de aplicação do legítimo interesse, eles não solucionam outras situações mais delicadas e logo conduzem à necessidade de uma análise extremamente casuística.

Logo, ao mesmo tempo em que os estudos das origens, fundamentos e aplicação do legítimo interesse na União Europeia nos dão maior conhecimento sobre o tema, possibilitando, potencialmente, a melhor aplicação do dispositivo no Brasil e garantindo uma uniformização que é necessária, eles apontam-nos também para a necessidade de a Agência Nacional de Proteção de Dados brasileira garantir a desburocratização e a especialização no preenchimento dos casos de interesse legítimo, de modo célere e não-judicial.

Conclui-se, portanto, pela necessidade de apreciação da matéria pela ANPD, de modo a promover a mais ampla e qualificada discussão sobre o assunto. Somente com uma regulamentação específica será possível colmatar o caráter perigosamente genérico do legítimo interesse no nosso ordenamento, impedindo iniquidades e promovendo uma tutela de proteção de dados efetiva no Brasil.

## REFERÊNCIAS

ALVES, Paulo. **O que é o Whois?** Disponível em: <https://www.techtudo.com.br/noticias/noticia/2015/03/o-que-e-whois.html>. Acessado em: 30 out. 2019.

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**. Adotado em 9 de abril de 2014. Disponível em: <https://www.dataprotection.ro/servlet/ViewDocument?id=1086>. Acesso em: 11 out. 2019.

BALBONI, Paolo. COOPER, Daniel. IMPERIALI, Rosario. MACENAITE, Milda. Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection. **International Data Privacy Law**, 2013.

BANISAR, David. DAVIES, Simon. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, And Surveillance Laws and Developments. **The John Marshall Journal of Computer & Information Law**, 1999.

BENNETT, Colin. Regulating Privacy: data protection and public policy in Europe and the United States. Ithaca: **Cornell University Press**, 1992.

BERBERET, Lúcia. **“Interesse legítimo” supera “consentimento” no tratamento de dados pessoais pelas empresas**. Disponível em: <<http://www.telesintese.com.br/interesse-legitimo-supera-consentimento-no-tratamento-de-dados-pelas-empresas/>>. Acesso em: 10 set. 2019.

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

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília, DF: ENDC, 2010. (Caderno de Investigações Científicas, v. 2). Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-deprotecao-de-dados-pessoais.pdf>. Acesso em: 25 out. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível: <[www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 20 ago. 2019.

CACHAPUZ, Maria Cláudia Mércio. Privacidade, proteção de dados e autodeterminação informativa. **Revista Jurídica da Presidência**, Brasília, DF, v. 15. n. 107, p. 823-848, out. 2013/jan. 2014.

COMISSÃO EUROPEIA. **Primeiro relatório sobre a implementação da directiva relativa à protecção de dados (95/46/CE)**, COM/2003/0265 final. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52003DC0265&from=EN>>. Acesso em: 27.10.2019.

CORDEIRO, A. Barreto Menezes. O tratamento de dados pessoais fundado em interesses legítimos. **Revista de direito e tecnologia**, Lisboa, vol. 1 (2019), no. 1, p. 1-31.

DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**. Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=pt>. Acesso em: 12 out. 2019.

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

DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 120/2018.

DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor**. São Paulo, v. 120/2018. p. 469-483.

FERRETTI, Federico. Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? **Common Law Market Review** 51, 2014.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. São Paulo: **Revista dos Tribunais**, 2019.

FUTURE OF THE PRIVACY FORUM; NIMITY PRIVACY COMPLIANCE SOFTWARE. **Processing personal data on the basis of Legitimate Interests under the GDPR: Practical cases**. Disponível em: <[https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20FPF%20-%20Legitimate%20Interests%20Report/Deciphering\\_Legitimate\\_Interests\\_Under\\_the\\_GDPR.pdf?hsCtaTracking=9cf491f2-3ced-4f9c-9ffa-5d73a77a773e%7C7469b2ec-e91c-4887-b5db-68d407654e23](https://info.nymity.com/hubfs/Landing%20Pages/Nymity%20FPF%20-%20Legitimate%20Interests%20Report/Deciphering_Legitimate_Interests_Under_the_GDPR.pdf?hsCtaTracking=9cf491f2-3ced-4f9c-9ffa-5d73a77a773e%7C7469b2ec-e91c-4887-b5db-68d407654e23)>. Acesso em: 10 out. 2019.

ICANN. **Sobre a ICANN**. Disponível em: <http://icannlac.org/PO/sobre-ICANN>. Acesso em: 30 out. 2019.

KAMARA, Irene. DE HERT, Paul. Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach. **The Cambridge handbook of consumer privacy**. 2018, p. 321-352.

MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. LGPD: Lei Geral de Proteção de Dados comentada. Viviane Nóbrega Maldonado, Renato Opice Blum, coordenadores. São Paulo: **Revista dos Tribunais**. 2019.

MAYER-SCHÖNBERGER, Victor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: **The Mit Press**, 2001.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, São Paulo, v. 79, p. 45-82, jul./set. 2011.

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

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**. vol. 1009/2019. 2019.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICOS (OCDE). **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais**. 1980. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 25 out. 2019.

THE ECONOMIST. Londres: **The Economist Group**. The world's most valuable resource is no longer oil, but data. 6 de maio de 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 10 set. 2019.

UK INFORMATION COMMISSIONER OFFICE. **Guide to the general data protection regulation** (GDPR). Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>. Acesso em: 11 out. 2019.

UNIÃO EUROPEIA. Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal: **Conselho da Europa**, Estrasburgo, 28 jan. 1981. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 10 out. 2019.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 20 set. 2019.

UNIÃO EUROPEIA. Regulamento Geral de Proteção de Dados (RGPD) 2015/679/CE, de 27 de abril de 2016. Disponível em: <<https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 20 out. 2019.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. Dissertação (Mestrado em Direito, Estado e Sociedade) – Faculdade de Direito, Universidade de Brasília, Brasília, DF, 2007. Disponível em: [repositorio.unb.br/bitstream/10482/3358/1/2007\\_TatianaMaltaVieira.pdf](http://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf). Acesso em: 12 out. 2019.

VOIGT, Paul. BUSSCHE, Axel von dem. The EU General Data Protection Regulation (GDPR): A practical guide. Springer, **Berlin Springer International Publishing Springer**, 2017.

ZANFIR-FORTUNA, Gabriela et al. Processing personal data on the basis of legitimate interests under the GDPR: practical cases. **Future of Privacy Forum**, 2018.