UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO

JULIA FREITAS FAZENDA

POSSÍVEIS CRITÉRIOS PARA A EXIGÊNCIA DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS A PARTIR DE UMA ANÁLISE COMPARADA

PORTO ALEGRE
2022
JULIA FREITAS FAZENDA

POSSÍVEIS CRITÉRIOS PARA A EXIGÊNCIA DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS A PARTIR DE UMA ANÁLISE COMPARADA

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharela em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientadora: Profª. Drª. Lisiane Feiten Wingert Ody.

PORTO ALEGRE
2022

JULIA FREITAS FAZENDA

POSSÍVEIS CRITÉRIOS PARA A EXIGÊNCIA DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS A PARTIR DE UMA ANÁLISE COMPARADA

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharela em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Aprovado em 06 de maio de 2022.

BANCA EXAMINADORA

_____

Profª. Dra. Lisiane Feiten Wingert Ody
Universidade Federal do Rio Grande do Sul (orientadora)

_____

Profª. Dra. Maria Claudia Cachapuz
Universidade Federal do Rio Grande do Sul

_____

Anita Spies Cunha
Universidade Federal do Rio Grande do Sul

AGRADECIMENTOS

À minha família, pelo apoio e suporte incondicionais ao longo de toda a minha trajetória e durante toda a minha vida. Vocês são meu porto seguro e sem vocês nada eu seria. Obrigada.

Aos meus amigos, por serem a família que eu escolhi. Compartilhar a vida com vocês me faz mais feliz. Muito obrigada por tanto.

À minha querida professora orientadora, Dra. Lisiane Feiten Wingert Ody, por todo o conhecimento compartilhado. És um exemplo de profissional que, além de inquestionável qualidade técnica, mantém a humanidade no exercício da docência. És fonte de admiração e inspiração.

Ao Henrique, pelo incansável apoio ao longo de todo o desenvolvimento do presente trabalho. Obrigada por ser minha melhor companhia e maior incentivador.

A todos os professores, colegas e chefes que contribuíram com o meu desenvolvimento pessoal e profissional.

RESUMO

A proteção de dados no Brasil é regulamentada pela Lei Geral de Proteção de Dados (LGPD). Entre as inúmeras orientações e obrigações dispostas ao longo da LGPD, no artigo 38 da Lei encontra-se a previsão de possível exigência, pela Autoridade Nacional de Proteção de Dados (ANDP), de Relatório de Impacto à Proteção de Dados a ser elaborado pelo Controlador das operações de tratamento de dados. Considerando a ausência de regulamentação específica sobre os Relatórios de Impacto pela Autoridade Nacional de Proteção de Dados (ANPD), a presente monografia, por meio de revisão bibliográfica e método comparativo funcional, objetiva identificar quais seriam os possíveis critérios para a exigência do documento pela Autoridade Nacional. Verifica-se que, nos moldes da legislação europeia, que regulamentou a matéria a partir do *General Data Protection Regulation* (GDPR), a LGPD optou por uma metodologia baseada em risco para a definição das hipóteses de tratamento de dados que demandariam a elaboração de Relatórios de Impacto. Assim, a partir de uma análise sistemática da experiência europeia no desenvolvimento do tema, bem como dos contornos brasileiros existentes, conclui-se que é possível a utilização, pela ANPD, da metodologia adotada na experiência europeia como subsídio para regulamentação do tema no contexto nacional. Busca-se, a partir do presente estudo, contribuir com o desenvolvimento do tema no contexto brasileiro de proteção de dados, a fim de conferir maior segurança jurídica aos agentes de tratamento de dados.

Palavras-chave: Proteção de Dados Pessoais; Relatório de Impacto; *Data Protection Impact Assessment*; Lei Geral de Proteção de Dados; *General Data Protection Regulation*.

ABSTRACT

Data protection subject in Brazil is regulated by the “Lei Geral de Proteção de Dados (LGPD)”. Among the numerous guidelines and obligations established throughout the LGPD, the Article 38 provides that the National Agency of Data Protection may require a Data Protection Impact Assessment from the data Controllers. Considering the absence of specific regulation on Data Protection Impact Assessment by the National Agency, this monograph, based on bibliographic review and functional comparative method, aims to identify what could be the possible criteria for the requirement of the document by the National Agency. As in the GDPR, the LGPD opted for a risk-based methodology to define which data treatment hypotheses would require the elaboration of Data Protection Impact Assessment. Considering the systematic analysis of the European experience in developing the theme, as well as the existing Brazilian orientation, the National Agency can use the methodology developed by the European experience to regulate the theme in the national context. This study seeks to contribute for the development of the topic in the Brazilian context of Data Protection, in order to provide legal security to data controllers.

Keywords: Data Protection; Data Protection Impact Assessment; Lei Geral de Proteção de Dados; General Data Protection Regulation.

SUMÁRIO

1 INTRODUÇÃO

Atualmente, o principal recurso propulsor da economia é a circulação de informação. A informação é, inclusive, adjetivo comumente utilizado para descrever o estágio atual da sociedade, caracterizada como “sociedade da informação”[1]. Nesse cenário, os dados pessoais são importantes fontes de geração de riqueza, visto que, uma vez processados, são capazes de traduzir informações extremamente relevantes sob o ponto de vista econômico[2].

Nesse contexto, e sendo a ciência jurídica uma ciência social que deve acompanhar o desenvolvimento dinâmico da sociedade, surgiu a necessidade de adequação das categorias jurídicas de modo a regulamentar os novos desafios relacionados a um contexto de tratamento massivo de dados pessoais[3].

Foi nesse cenário de desenvolvimento social e econômico que surgiram legislações destinadas a tutelar a proteção dos dados pessoais dos indivíduos, de modo a criar limites para o uso, processamento, compartilhamento e quaisquer outras espécies de tratamento de dados pessoais[4], assim como instituir obrigações relacionadas à identificação e à mitigação de riscos associados ao tratamento de dados. No contexto brasileiro, a matéria é regulamentada pela Lei Geral de Proteção de Dados (LGPD).

A LGPD dispõe sobre o tratamento de dados pessoais realizado por pessoas naturais ou jurídicas, com o objetivo de tutelar a liberdade, privacidade e livre desenvolvimento da pessoa[5]. A legislação prevê princípios e fundamentos para o tratamento de dados pessoais, apresenta diretrizes e orientações a serem observadas

---

1 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 4-5.

2 FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 23-52.

3 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 4-5.

4 A partir de um conceito expansionista, adotado pelo Brasil, dado pessoal é todo o tipo de informação relacionada a uma pessoa natural identificada ou identificável (MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019, p. 89).

5 Art. 1º, *caput* (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

e obrigações a serem cumpridas por entes que realizem o tratamento de dados pessoais.

Entre as inúmeras orientações e obrigações dispostas ao longo da LGPD, no artigo 38 da Lei encontra-se a previsão de possível exigência, pela Autoridade Nacional de Proteção de Dados (ANDP), de Relatório de Impacto à Proteção de Dados a ser elaborado pelo Controlador[6].

Além da referência no artigo acima indicado, o Relatório de Impacto à Proteção de Dados Pessoais é expressamente mencionado, de forma sucinta, em algumas outras oportunidades ao longo da legislação, sendo importante fazer referência a algumas delas.

O artigo 5º, inciso XVII, da LGPD traz a definição do Relatório de Impacto como a documentação do Controlador destinada a descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, além de indicar medidas, salvaguardas e mecanismos para a mitigação de tais riscos[7]. No artigo 4º, § 3º, é referido que a ANPD poderá exigir o Relatório de Impacto quando o tratamento de dados pessoais se enquadrar em uma das exceções de aplicação da LGPD elencadas no inciso III do *caput* do mesmo artigo[8].

O artigo 10, § 3º, LGPD, por sua vez, prevê que a ANPD poderá solicitar o documento dos controladores quando o tratamento de dados tiver como fundamento o legítimo interesse[9]. Já o artigo 55-J, inciso XIII, LGPD, preceitua que cabe à ANPD elaborar regulamentos sobre o Relatório de Impacto à Proteção de Dados Pessoais

---

6 "Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

7 Art. 5º, XVII (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

8 Art. 4º, §3º (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

9 Art. 10, §3º (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

para os casos de tratamentos de dados que representem alto risco à garantia dos princípios gerais de proteção de dados previstos na LGPD[10].

No entanto, apesar das vagas referências sobre quando o Relatório de Impacto pode ser necessário, o texto legal deixou em aberto a definição das hipóteses em que o documento pode ser exigido dos controladores, lacuna que, segundo a própria legislação, deve ser preenchida por regulamentação a ser expedida pela ANPD.

Já no que se refere à atuação da Autoridade Nacional, até o momento de escrita da presente monografia, a ANPD não expediu regulamentação específica sobre os Relatórios de Impacto, sendo que a sua atuação, até então, se resume à realização de reuniões técnicas sobre a temática, sem qualquer definição concreta sobre a matéria.

E é justamente na lacuna de orientação sobre o tema pela ANPD, e consequente ausência de segurança jurídica enfrentada pelos agentes de tratamento de dados, que se encontra a relevância do tema do presente trabalho[11]. Por meio de revisão bibliográfica e método comparativo funcional, a pesquisa busca identificar quais seriam os possíveis critérios para a exigência do documento pela ANPD.

Para possibilitar a análise a que se propõe, o presente trabalho examina, na primeira parte do seu desenvolvimento, a forma como a União Europeia vem abordando a temática e, na segunda parte do desenvolvimento, o que a legislação brasileira, interpretações doutrinárias nacionais e orientações da ANPD podem indicar como solução para a questão no contexto brasileiro.

Preliminarmente, entende-se necessário justificar a opção pela análise comparada com o direito europeu, motivo pelo qual as próximas linhas se ocuparão a, em um primeiro momento, abordar alguns dos pontos de convergência que

---

[10] Art. 55-J, XIII (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

[11] A necessidade de orientação específica sobre o tema se justifica nas potenciais consequências negativas da ausência de quaisquer critérios preestabelecidos para as hipóteses de exigência do relatório de impacto. Isso porque tal situação pode levar à onerosidade excessiva dos agentes de tratamento que, para se protegerem de eventuais sanções por descumprimento da LGPD, optam por elaborar relatórios de impacto para todas as operações de tratamento de dados identificadas em suas operações. E, em razão da complexidade inerente à elaboração do relatório de impacto, corre-se o risco de os agentes de tratamento elaborarem documentos “pro forma”, o que, por sua vez, acaba por banalizar o relatório de impacto e desviar sua real finalidade. Sobre o assunto ver: TIMM, Luciano; CAOVILLA, Renato; STURARI, Mateus. O Relatório de Impacto na LGPD: Sentido e Limites Dentro da Regulação Econômica. *In*: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coords.). **Proteção de Dados:** Temas Controvertidos. Indaiatuba: Editora Foco, 2021, pp. 362-384.

aproximam a legislação brasileira de proteção de dados (LGPD) da legislação europeia, o Regulamento Geral sobre a Proteção de Dados (em inglês, "*General Data Protection Regulation*", comumente conhecido por sua sigla "GDPR"), e, em um segundo momento, enfrentar a equivalência entre o Relatório de Impacto à Proteção de Dados Pessoais brasileiro e o "*Data Protection Impact Assessment*" (DPIA).

Apesar de contarem com técnicas legislativas distintas, tendo em vista que a LGPD é menos prescritiva e não contém considerandos[12] como diretrizes para interpretação do texto legal da forma como o GDPR possui[13], a lei brasileira foi, desde o princípio, inspirada no modelo europeu de proteção de Dados[14], especialmente no GDPR.

Essa inspiração pode ser facilmente identificada nos diversos pontos de convergência entre as legislações, a começar pela exigência, em ambos os casos, de uma base legal para o tratamento de dados pessoais, e, mais do que isso, a definição de bases legais extremamente semelhantes entre si. Verifica-se que a LGPD possui as mesmas bases legais definidas pelo GDPR, contando apenas com o acréscimo de 4 novas bases. São bases legais comuns entre as legislações: i) consentimento; ii) execução de contrato do qual o titular faça parte; iii) cumprimento de obrigação legal; iv) tutela da vida do titular ou de outra pessoa natural; v) execução de políticas públicas; e vi) atendimento de interesses legítimos do responsável pelo tratamento ou terceiro[15].

Além disso, a semelhança entre a LGPD e o GDPR é clara em outros pontos, como nos princípios gerais elencados para orientar o tratamento de dados pessoais, existência de regras especiais para o tratamento de dados pessoais sensíveis, criação

---

12 "Considerandos" é a tradução técnica para "*recitals*".

13 BIONI, Bruno Ricardo; GOMES, Maria Cecilia Oliveira; MONTEIRO, Renato Leite. GDPR matchup: Brazil's General Data Protection Law. **IAPP,** Portsmouth, 04 out. 2019. Disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Acesso em: 22 abr. 2022.

14 DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, nov./dez. 2018.

15 Art. 6º (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022). E também: Art. 7º (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

de autoridade para a regulamentação da aplicação da lei e, também, diferentes responsabilidades atribuídas às figuras de controlador e operador de dados[16].

Também há clara convergência nas disposições sobre os direitos dos titulares previstos na LGPD e no GDPR, especificamente no que se refere ao direito de acesso, notificação e retificação dos dados, cancelamento do tratamento e portabilidade de dados. Ainda, no GDPR esses direitos estão previstos no capítulo 3 da lei, curiosamente no mesmo número do capítulo destinado à tutela dos direitos dos titulares na LGPD[17].

A forma semelhante como ambas as legislações regulam as decisões automatizadas, de modo a resguardar os direitos dos titulares de explicação e possibilidade de auditoria no caso de potencial discriminatório resultante de tratamento automatizado de dados pessoais, e, ainda, a adoção, por ambas as legislações, de um modelo *ex ante* de proteção de dados, são, também, pontos de aproximação entre as leis[18].

Além de todos os aspectos mencionados, o mais relevante para justificar a opção pela análise comparada no presente trabalho é adoção, pela LGPD, de um instrumento de avaliação de impacto à proteção de dados exatamente na linha daquele previsto pelo GDPR[19].

---

16 DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, nov./dez. 2018.

17 BIONI, Bruno Ricardo; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 791-814, p. 802.

18 BIONI, Bruno Ricardo; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 791-814, p. 803-804.

19 "Art. 5º: Para os fins desta Lei, considera-se: [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022). E também: "*Article 35. 1- Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks*" (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022).

Na esteira da regulamentação europeia, a LGPD adota o princípio da *accountability* (“prestação de contas”), apostando na colaboração dos agentes de tratamento de dados na mitigação dos riscos das suas próprias atividades. As principais ferramentas para concretização de tal princípio e viabilização da mitigação de riscos das atividades previstas nas legislações de proteção de dados são o Relatório de Impacto à Proteção de Dados Pessoais (LGPD) e o *Data Protection Impact Assessment*” (GDPR), documentos destinados a descrever e mitigar os riscos de processos de tratamento de dados que possam gerar riscos para os titulares de dados[20].

Sendo a função do Relatório de Impacto à Proteção de Dados Pessoais brasileiro a mesma assumida pelo *Data Protection Impact Assessment,* resta justificada a opção pela análise das orientações europeias sobre o documento para fins de identificar parâmetros que possam ser adotados pela Autoridade Nacional Brasileira de Proteção de Dados na regulamentação da matéria.

Isso porque, enquanto a legislação brasileira não prevê parâmetros para identificação das hipóteses nas quais o relatório de impacto poderá ser exigido, a regulamentação europeia conta com um capítulo próprio destinado a apontar em que casos o documento é obrigatório, além de contar com considerandos que abordam importantes definições e conceituações essenciais para a interpretação acerca da necessidade de elaboração do documento[21].

E, além das prescrições constantes no texto legal do GDPR, a União Europeia, em razão da sua cultura de proteção de dados mais consolidada, também já desenvolveu importantes orientações que identificam hipóteses nas quais o processamento de dados pode ser considerado de “alto risco” para os fins do GDPR e, portanto, demandar a elaboração de relatórios de impacto. O principal documento orientativo é aquele emitido pelo *Article 29 Working Party* denominado “*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is*

---

[20] BIONI, Bruno Ricardo; MENDES, Laura Schertel. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, pp. 157-180, jul./ago. 2019.

[21] BIONI, Bruno Ricardo; MENDES, Laura Schertel. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, pp. 157-180, jul./ago. 2019.

"likely to result in a high risk" for the purposes of Regulation 2016/679"[22]. Nessa mesma linha, existem, também, *blacklists* e *whitelists* desenvolvidas pelas autoridades nacionais de diferentes países da União Europeia, destinadas a complementar o rol exemplificativo trazido pelo *Article 29 Working Party* e indicar hipóteses que também podem ser enquadradas como tratamento de alto risco (*blacklists*) e tratamento de baixo risco (*whitelists*).

Ou seja, a significativa convergência entre as legislações brasileira (LGPD) e europeia (GDPR) de proteção de dados, especialmente no que se refere à criação, por ambas, de documentos de análise de impacto à proteção de dados, somada à existência de documentos e parâmetros mais definidos no direito europeu sobre quando seria necessário elaborar tais documentos, justificam a pertinência da análise da experiência europeia para identificação de parâmetros que podem ser também utilizados na realidade brasileira.

Já a relevância da segunda parte do desenvolvimento da presente monografia reside na necessidade de identificação do que pode ser utilizado da experiência europeia no contexto brasileiro, a partir de uma análise mais aprofundada e atenta da experiência nacional na regulamentação da temática.

Assim, a partir da análise dos critérios adotados no âmbito da União Europeia para a definição de hipóteses de exigência do relatório de impacto, o presente estudo se propõe a identificar possíveis parâmetros para a regulamentação do tema no contexto brasileiro.

Feitos os esclarecimentos preliminares e contextualização do tema, passa-se ao primeiro capítulo do trabalho.

---

[22] UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

2 *DATA PROTECTION IMPACT ASSESSMENT* E SUA REGULAMENTAÇÃO NA UNIÃO EUROPEIA

O presente capítulo se propõe a analisar a regulamentação do *Data Protection Impact Assessment* (DPIA) no âmbito da União Europeia, especificamente no que se refere às hipóteses em que a elaboração do documento pelos agentes de tratamento de dados se faz necessária.

Para isso, enfrenta-se, em um primeiro momento, as disposições legais sobre o tema constantes no GDPR. Em um segundo momento, busca-se explorar o desenvolvimento do tema em documentos expedidos pelo órgão consultivo da União Europeia *Article 29 Working Party*. E, em um terceiro momento, passa-se a analisar o histórico das sanções administrativas relacionadas à ausência de elaboração de relatório de impacto no âmbito da União Europeia, a fim de visualizar como as autoridades nacionais têm exigido, na prática, a elaboração do documento dos agentes de tratamento.

Ainda, importante destacar que, em que pese a tradução literal de *Data Protection Impact Assessment* seja “Avaliação de Impacto à Proteção de Dados”, como o documento equivale ao relatório de impacto brasileiro, conforme abordado na introdução do presente estudo, por vezes, ao longo do presente capítulo, o documento será referido como “relatório de impacto”, ou apenas “DPIA” (sigla de *Data Protection Impact Assessment*), a fim de facilitar a referência ao documento e, também, a analogia ao relatório de impacto brasileiro.

2.1 O GDPR NA REGULAMENTAÇÃO DO TEMA

Antes de analisar as disposições normativas constantes no GDPR a respeito do *Data Protection Impact Assessment*, aborda-se, preliminarmente, a estrutura normativa do Regulamento Europeu.

O GDPR é bastante prescritivo, organizado em diversos “níveis”, que vão desde a previsão de garantias fundamentais amplas, passando pela exposição de definições de conceitos-chave, até a prescrição de normas e orientações específicas aos agentes de tratamento de dados, como medidas de *compliance*[23].

[23] POLIDO, Fabricio *et. al.* **GDPR e suas repercussões no direito brasileiro**: primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade – IRIS: Belo Horizonte,

Além dos 90 artigos que constituem os requisitos legais a serem obrigatoriamente observados pelas organizações para sua adequação ao GDPR, o Regulamento também conta com 173 considerandos, que fornecem informações adicionais e contextualização suporte para os artigos legais[24]. Nesse sentido, os considerandos do GDPR estipulam parâmetros interpretativos para as disposições legais e, muitas vezes, abordam importantes definições e esclarecimentos conceituais que serão importantíssimos quando da efetivação e aplicação das normas.

Ultrapassada a compreensão preliminar da estrutura normativa do GDPR, passa-se à análise das disposições legais que tratam sobre o DPIA na legislação europeia objeto de estudo.

O artigo 35 do GDPR dispõe sobre o *Data Protection Impact Assessment* e prevê, em seu parágrafo primeiro, que o documento deverá ser elaborado pelo controlador nos casos em que o tratamento de dados for suscetível de implicar um elevado risco aos direitos e liberdades dos titulares, sendo particularmente importante quando se introduz uma nova tecnologia na operação, considerando a natureza, escopo e contexto do processamento[25].

A partir disso, verifica-se que o GDPR adotou a metodologia da avaliação de risco para a definição das hipóteses nas quais o relatório de impacto deve ser elaborado[26]. No entanto, para que exista maior grau de segurança jurídica, se faz necessário identificar situações mais concretas que podem implicar alto risco aos titulares e que, portanto, demandem a elaboração de relatório de impacto.

Isso porque, a definição de operação de tratamento de dados que seja suscetível de implicar um elevado risco aos direitos e liberdades dos titulares [27] é

2018, p. 08. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%c3%b5es-no-direito-brasileiro-Primeiras-impress%c3%b5es-de-an%c3%a1lise-comparativa-PT.pdf. Acesso em: 22 abr. 2022.

24 WILLS, Leonard. A Very Brief Introduction to the GDPR Recitals. **Minority Trial Lawyer**, v. 17, n. 1, p. 15-16, maio 2019. Disponível em: https://heinonline.org/HOL/Page?public=true&handle=hein.aba/mitril0017&div=8&start_page=15&collection=trials&set_as_cursor=0&men_tab=srchresults. Acesso em: 22 abr. 2022.

25 Artigo 35, 1 (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022).

26 GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In:* LIMA, Ana Paula; HISSA, Carmina; SALDANHA, Paloma Mendes (Orgs.). **Direito Digital:** Debates Contemporâneos. São Paulo: Revista dos Tribunais, 2019, pp. 141-153.

27 Artigo 35, 1 (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. Official Journal of the European Union, 04 maio 2016. Disponível em:

demasiadamente ampla e subjetiva, abrindo margem para múltiplas interpretações no campo prático.

Nesse sentido, ainda que de forma não taxativa, o próprio regulamento europeu apresenta, no parágrafo terceiro do artigo 35, algumas hipóteses nas quais a elaboração do relatório de impacto seria necessária[28], sendo elas: i) operações que envolvam sistemática e extensiva avaliação de aspectos pessoais relacionados a pessoas naturais que seja baseada em processos automatizados, incluindo a definição de perfis, e que produzam efeitos jurídicos às pessoas naturais ou que as afetem de forma similar; ii) operações de tratamento em larga escala de dados sensíveis ou de dados relacionados a condenações penais e infrações; e iii) operações que envolvam o monitoramento sistemático de uma área publicamente acessível em larga escala[29].

Além disso, preceitua, nos parágrafos quarto e quinto do mesmo artigo, que a autoridade de controle deverá estabelecer e tornar pública uma lista com os tipos de processos de tratamento de dados que estão sujeitos à exigência de elaboração de relatório de impacto e poderá, também, estabelecer e tornar pública uma lista com os tipos de operações de processamento de dados que não demandam a elaboração do relatório de impacto[30].

No entanto, apesar da previsão de algumas hipóteses de exigência do documento no texto do artigo 35 do GDPR, especialmente em seu parágrafo terceiro, a identificação, na prática, de situações que poderiam estar abarcadas pelo dispositivo é bastante subjetiva e, consequentemente, difícil, se considerado apenas o texto normativo.

Por exemplo, o que seria considerado como “sistemática e extensiva avaliação de aspectos pessoais de pessoas naturais” ou o que seriam considerados “efeitos

---

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022).

28 TIMM, Luciano; CAOVILLA, Renato; STURARI, Mateus. O Relatório de Impacto na LGPD: Sentido e Limites Dentro da Regulação Econômica. *In*: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coords.). **Proteção de Dados:** Temas Controvertidos. Indaiatuba: Editora Foco, 2021, pp. 362-384, p. 370.

29 Artigo 35 (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022)

30 Artigo 35, 4 e 5 (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022).

jurídicos” causados por operações de tratamento, para fins de observância do disposto no item (a) do parágrafo terceiro do artigo 35 do GDPR? Ainda, o que seriam tratamentos de larga escala e qual deve ser a métrica a ser considerada para classificar uma operação como de larga escala, para os fins do item (b) do artigo 35 do GDPR? Que tipos de áreas poderiam ser enquadradas como publicamente acessíveis para fins do item (c) do artigo 35 do GDPR? Além disso, como o parágrafo terceiro do artigo 35 do GDPR não se trata de um rol taxativo de hipóteses de exigência do relatório de impacto, quais seriam as outras situações que poderiam causar risco aos direitos e liberdades dos titulares?

A fim de elucidar a aplicação dessas disposições do GDPR, o próprio regulamento explorou alguns conceitos importantes para a interpretação dos dispositivos normativos nos seus considerandos.

Os considerandos relacionados ao artigo 35 do GDPR são os de números 75, 84, 89, 90, 91, 92 e 93, e aqueles que apresentam definições relevantes especificamente para fins de identificação das hipóteses de exigência do relatório de impacto são os de números 75, 89 e 91, que conceituam operações de tratamento de dados que podem causar riscos aos direitos e liberdades dos titulares, bem como operações de tratamento classificadas como de larga escala[31].

No entanto, apesar de fornecerem parâmetros mais detalhados para interpretação e identificação de hipóteses de tratamento de dados que demandariam

[31] O considerando nº 75 do GDPR refere que operações de tratamento de dados que causariam riscos aos direitos e liberdades de pessoas naturais resultariam de operações suscetíveis de causar danos físicos, materiais ou imateriais aos titulares, em especial quando o tratamento possa dar origem à discriminação, usurpação ou roubo da identidade, perdas financeiras, prejuízos para reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, inversão não autorizada de pseudonimização ou quaisquer outros danos de natureza econômica ou social, tratamentos que possam ocasionar privação dos titulares de dados de seus direitos, impedimento do exercício de controle sobre os seus respectivos dados pessoais, tratamento de dados sensíveis dos titulares ou referentes a condenações penais ou infrações, bem como tratamento de dados de pessoas vulneráveis e operações que envolvem a avaliação de aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais, ao comportamento, ao deslocamento e localização das pessoas, a fim de definir perfis. O Considerando nº 89 do GDPR, por sua vez, complementa que operações de tratamento que envolvam o uso de novas tecnologias também podem resultar em alto risco aos direitos e liberdades dos titulares. Por fim, o Considerando nº 91 refere a necessidade de elaboração de relatório de impacto nas operações de tratamento de dados de larga escala que envolvam o tratamento de grande quantidade de dados pessoais a nível regional, nacional ou supranacional e possam afetar um número considerável de titulares de dados, além de serem suscetíveis de implicar um elevado risco em razão da sua sensibilidade ou nos quais seja utilizada nova tecnologia, bem como operações que dificultem o exercício, pelos titulares, de seus direitos. (UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados (RGPD, GDPR)**. Considerandos n. 75, 89 e 91. Bruxelas, 2018. Disponível em: https://gdpr-text.com/pt/read/article-35/#recital. Acesso em: 22 abr. 2022).

a elaboração de relatório de impacto, os considerandos do GDPR não são capazes de preencher todas as lacunas sobre a temática, deixando espaço para que órgãos regulamentadores esclareçam e explorem, de forma mais detalhada e prática, a matéria.

Nesse sentido, um dos principais documentos de reforço acerca do tema foi o trabalho do *Article 29 Working Group*[32], o qual é analisado de forma mais aprofundada no próximo subcapítulo.

2.2 O DESENVOLVIMENTO DO TEMA PELO ÓRGÃO CONSULTIVO DA UNIÃO EUROPEIA *ARTICLE 29 WORKING PARTY*

No presente subcapítulo, passa-se a analisar as diretrizes traçadas pelo *Article 29 Working Party* no que se refere à elaboração do relatório de impacto pelos agentes de tratamento de dados.

2.2.1 *Article 29 Working Party*

Previamente à análise dos documentos expedidos pelo órgão consultivo da União Europeia, necessário esclarecer do que se trata o *Article 29 Working Party* e o porquê da relevância dos trabalhos que realizou.

"Article 29 Working Party" é o Grupo de Trabalho do Artigo 29, órgão independente da União Europeia que lidou com questões relativas à proteção da privacidade e dos dados pessoais até maio de 2018, data da entrada em vigor do GDPR[33]. A partir de maio de 2018, o órgão foi substituído pelo Conselho Europeu de Proteção de Dados (*European Data Protection Board* - EDPB), órgão europeu independente, sediado em Bruxelas, que contribui para a aplicação das regras de

---

[32] GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In:* LIMA, Ana Paula; HISSA, Carmina; SALDANHA, Paloma Mendes (Orgs.). **Direito Digital:** Debates Contemporâneos. São Paulo: Revista dos Tribunais, 2019, pp. 141-153.

[33] Sobre a definição, ver website do European Data Protection Board (Sobre a definição, ver website do European Data Protection Board. UNIÃO EUROPEIA. Comissão Europeia. Article 29 Working Party. **European Data Protection Board**. Bruxelas, [*s.d*.]. Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en. Acesso em: 22 abr. 2022).

proteção de dados em toda a União Europeia e promove cooperação entre as Autoridades de Proteção de Dados da União Europeia[34].

O Grupo de Trabalho do Artigo 29 era composto por um representante da autoridade de controle indicado por cada país membro da União Europeia, um representante da autoridade criada para as instituições e organizações da União Europeia e um representante da Comissão Europeia[35].

O órgão contou com elevada qualidade técnica e foi responsável por elaborar diversos guias orientativos extremamente relevantes para o auxílio na interpretação e aplicação do GDPR. Entre tais documentos, merece destaque para fins da análise do presente trabalho o "*Guidelines on Data Protection Impact Assessment (DPIA)"*, que contém importantes diretrizes interpretativas para definição das hipóteses nas quais se faz necessária a elaboração de relatórios de impacto e o "*Guidelines on Data Protection Officers",* que apresenta importantes definições sobre o tratamento de dados em larga escala, que podem ser consideradas para fins de complementação do entendimento a respeito do tema objeto do presente estudo.

2.2.2 *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*

O trabalho do *Article 29 Working Party* sobre o relatório de impacto foi um dos principais reforços em relação ao tema. O órgão, em 2017, elaborou o "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk for the purposes of Regulation 2016/679*", um guia orientativo que contém importantes diretrizes interpretativas e esclarecimentos a respeito do relatório de impacto, solidificando as hipóteses nas quais o *Data Protection Impact Assessment* seria obrigatório. As situações apontadas no documento

---

[34] Sobre a definição, ver website do European Data Protection Board (UNIÃO EUROEIA. Who we are. **European Data Protection Board.** Bruxelas, [*s.d*.]. Disponível em: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en. Acesso em: 22 abr. 2022).

[35] Sobre a definição, ver website da European Commission (UNIÃO EUROPEIA. **Article 29 working party, composition & structure**. Bruxelas, 06 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/605262/en. Acesso em: 22 abr. 2022).

esclarecem o que seria considerado um tratamento suscetível de resultar em elevado risco para fins de obrigatoriedade de elaboração de relatório de impacto[36].

O guia orientativo é dividido em quatro capítulos e contém dois anexos. O primeiro capítulo é a introdução, que apresenta a definição do *Data Protection Impact Assessment* (DPIA) como um processo destinado a descrever o processamento de dados pessoais, avaliar sua necessidade e proporcionalidade e ajudar a administrar os riscos que a operação de tratamento de dados gera aos direitos e liberdades dos titulares por meio da sua avaliação e previsão de medidas para sua mitigação. Resume a definição do DPIA como um processo para construir e demonstrar *compliance* com o GDPR. Ainda, aponta que a não elaboração de DPIA quando necessário pode resultar na aplicação de multas pela autoridade competente[37].

O segundo capítulo do documento é destinado a abordar o escopo de aplicação do guia orientativo e apresenta importantes esclarecimentos acerca do próprio objetivo do guia orientativo, demonstrando a sua relevância para o desenvolvimento do tema[38].

Refere-se, na oportunidade, que o documento se propõe a elucidar a noção de processos suscetíveis de causar risco elevado aos direitos e liberdades dos titulares, a fim de conceder uma interpretação consistente às hipóteses nas quais a elaboração do DPIA é obrigatória e fornecer critérios para as listas que seriam adotadas pelas autoridades de proteção de dados sobre o artigo 35 do GDPR[39].

Nessa linha, o documento também busca promover o desenvolvimento de uma lista comum para a União Europeia contendo: i) processos de tratamento de dados para os quais a elaboração de um DPIA é obrigatória; ii) processos de tratamento de dados para os quais a elaboração de um DPIA não é obrigatória; iii) critério comum

---

36 GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In:* LIMA, Ana Paula; HISSA, Carmina; SALDANHA, Paloma Mendes (Orgs.). **Direito Digital:** Debates Contemporâneos. São Paulo: Revista dos Tribunais, 2019, pp. 141-153.

37 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

38 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

39 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

de metodologia para elaboração de um DPIA; iv) critério comum que especifique quando a autoridade deve ser consultada, nos termos do artigo 36 do GDPR; e v) recomendações, quando possível, com base nas experiências adquirida pelos Estados-membro da União Europeia[40].

Além dos esclarecimentos acerca dos objetivos do guia orientativo, também no segundo capítulo, há menção a documentos que foram considerados para a elaboração do guia em questão. Entre os documentos indicados, consta o "*Guidelines on Data Protection Officer 16/EN WP 243*", que é objeto de análise no subcapítulo seguinte do presente trabalho justamente por conter importantes diretrizes interpretativas sobre temas que se correlacionam com o objeto do presente estudo[41].

O terceiro capítulo do documento versa sobre o conteúdo propriamente dito do guia orientativo e está dividido em 5 subcapítulos, que buscam abordar, resumidamente: a) o que um DPIA aborda; b) quais operações de tratamento de dados estão sujeitas à elaboração de um DPIA; c) necessidade de DPIA para operações que já existem; d) como elaborar um DPIA; e e) quando a autoridade nacional de proteção de dados deve ser consultada[42].

Após, é apresentada a conclusão e recomendações, no quarto capítulo do documento. Como anexos, apresenta-se exemplos de modelos de DPIAs e critérios para um DPIA aceitável[43].

Como o objetivo do presente estudo é identificar hipóteses em que o relatório de impacto pode ser obrigatório, a análise mais detalhada limita-se às disposições do documento que versam especificamente sobre situações de exigência do relatório de impacto, constantes no subcapítulo "b" do capítulo três do guia orientativo.

---

40 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

41 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

42 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

43 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

O subcapítulo “b” do terceiro capítulo do documento se propõe a abordar as operações de tratamento de dados que estariam sujeitas a um relatório de impacto por serem suscetíveis de resultar em um elevado risco aos direitos e liberdades dos titulares[44]. Além da referência às hipóteses já identificadas pelo próprio artigo 35 do GDPR, o guia orientativo apresenta uma lista mais concreta de operações que demandariam a elaboração de um DPIA em decorrência de seu elevado risco. Para a formulação dessa lista, foram apontados nove critérios a serem considerados para a classificação das operações como suscetíveis de resultar em alto risco[45].

A esse respeito, inclusive, a *European Data Protection Board* confirmou a importância dos critérios do guia orientativo do *Article 29 Working Party* tanto para fins de implementação do artigo 35 do GDPR quanto para garantia de uma consistência no âmbito da União Europeia[46].

Alguns dos critérios fornecidos pelo documento consistem em formas específicas de realizar tratamento de dados. Nesse sentido, de acordo com o primeiro critério formulado, o guia orientativo considera de alto risco, com base nos considerandos 71 e 91 do GDPR, as operações de avaliação ou classificação, o que inclui a definição de perfis e previsões sobre os titulares dos dados, especialmente quando se refere a aspectos relacionados ao desempenho profissional, situação econômica, saúde, preferências pessoais ou interesses, confiabilidade ou comportamento, localização ou deslocamento[47]. Ou seja, operações que envolvam a construção de perfis dos indivíduos, o denominado “*profiling*”[48].

---

[44] UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

[45] TIMM, Luciano; CAOVILLA, Renato; STURARI, Mateus. O Relatório de Impacto na LGPD: Sentido e Limites Dentro da Regulação Econômica. *In*: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coords.). **Proteção de Dados:** Temas Controvertidos. Indaiatuba: Editora Foco, 2021, pp. 362-384, p. 373.

[46] GELLERT, Raphael. EDPB Opinion on the Draft Lists of Competent Supervisory Authorities regarding the Processing Operations Subject to DPIAs. **European Data Protection Law Review**, n. 4, pp. 500-504, Berlim, 2018.

[47] GELLERT, Raphael. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. **European Data Protection Law Review**, n. 2, pp. 212-217, Berlim, 2017.

[48] A respeito da definição de *profiling*, segundo o “*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”*, documento também elaborado pelo Article 29 Working Party, “*profiling”* é um procedimento que pode envolver uma série de deduções estatísticas. É frequentemente utilizado para realizar previsões sobre pessoas, utilizando diversas fontes para inferir alguma informação sobre um indivíduo, baseado em qualidades de outros que seriam estatisticamente similares. Como o GDPR define profiling como um processo automatizado de dados pessoais para avaliação de aspectos pessoais, em particular para analisar ou fazer previsões sobre indivíduos, tem-se que profiling envolve alguma forma de avaliação ou julgamento

A fim de fornecer parâmetros mais concretos para a identificação desse critério na prática das operações de agentes de tratamento, o guia orientativo apresenta alguns exemplos de operações que envolveriam a avaliação ou classificação, como a seleção de clientes realizada por instituições financeiras a partir de bases de dados de referências de crédito bancário, de lavagem de dinheiro ou financiamento ao terrorismo, operações realizadas por empresas de biotecnologia que ofereça teste genético de seus clientes como forma de avaliar e prever riscos de doenças ou para a saúde, ou, ainda, desenvolvimento de perfis comportamentais ou publicitários baseados na utilização ou navegação no site do agente de tratamento de dados[49].

De forma complementar aos exemplos trazidos pelo Guia Orientativo, em um exercício de abstração, é possível enquadrar no critério sob análise, também, operações que identificam padrões de consumo ou de interesse em produtos na internet, ferramenta muito utilizada nas redes sociais para fins de *marketing* dirigido, bem como avaliações de desempenho profissional realizadas por empresas em relação a seus colaboradores ou, ainda, testes de personalidade ou de vocação profissional, por exemplo.

Operações de tratamento que envolvem decisões automatizadas[50] com o objetivo de tomada de decisões a respeito dos titulares de dados, de modo a produzir efeitos legais ou similares às pessoas naturais são consideradas como um segundo

---

sobre uma pessoa. Nesse sentido, são apontados os seguintes elementos que compõem o profiling: i) deve ser um processamento automatizado de dados pessoais; ii) deve ser realizado com dados pessoais; e iii) o objetivo do profiling deve ser avaliar aspectos pessoais sobre uma pessoa natural. Assim, uma simples classificação dos indivíduos baseadas em características aparentes, como idade, gênero, altura, não necessariamente implica em profiling, o que dependerá do propósito da classificação. De uma forma geral, profiling significaria avaliar as características e padrões de comportamento de indivíduos a partir da reunião de informações sobre um indivíduo ou grupo de indivíduos a fim de incluí-los em uma categoria de grupo, particularmente a fim de analisar ou realizar previsões sobre a habilidade de responder uma prova, interesses pessoais ou comportamentos (UNIÃO EUROPEIA. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)**. Bruxelas, 22 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 22 abr. 2022).

[49] UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

[50] Também a partir da definição apresentada no documento "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679",* decisões automatizadas são decisões tomadas a partir de meios tecnológicos sem envolvimento humano, podendo ser baseadas em qualquer tipo de dado pessoal, o que contempla dados fornecidos pelos próprios titulares, dados que foram observados a respeito dos indivíduos ou dados inferidos ou derivados acerca de um indivíduo, como dados de perfis já traçados (UNIÃO EUROPEIA. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)**. Bruxelas, 22 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 22 abr. 2022).

critério pelo guia orientativo. Como exemplo, é mencionado o processamento de dados que pode conduzir à exclusão ou discriminação dos titulares dos dados. Nesse sentido, é esclarecido que processamento automatizado de dados com pequeno ou nenhum efeito sobre os indivíduos não está enquadrado no critério específico[51].

Como terceiro critério é apresentado o processamento de dados para fins de observação, controle ou monitoramento dos titulares dos dados, incluindo dados coletados a partir de redes de informações ou de um monitoramento sistemático de uma área publicamente acessível[52]. Tal forma de tratamento de dados é considera de alto risco pelo guia orientativo porque, nessas situações, além de não terem quaisquer informações relacionadas às formas de tratamento de seus dados, os titulares não têm como evitar tal tratamento[53].

A partir da definição apresentada no terceiro critério, é possível enquadrar nessa hipótese situações bastante corriqueiras, como o monitoramento de espaços publicamente acessíveis por câmeras de segurança, por exemplo. Isso porque, basta estar no ambiente que está sendo monitorado por câmeras de segurança para estar, automaticamente, sujeito a esse tipo de tratamento. Além disso, por vezes, o titular pode nem estar ciente sobre o monitoramento por imagens ou sobre quem é o responsável por tal espécie de tratamento de dados.

A noção de dados sensíveis também é enfrentada no documento como o quarto critério, o que englobaria, além dos dados classificados como sensíveis pelo artigo 9 do GDPR e dados relacionados a condenações criminais, conforme definido no artigo 10 do GDPR, dados que seriam sensíveis em razão do contexto no qual são usados. O *Article 29 Working Party* esclarece que não necessariamente o tratamento de dados sensíveis significaria um alto risco da operação, vez que dependeria do contexto, como, por exemplo, se os dados já estavam publicamente disponíveis ou se o tratamento de dados condiz com as expectativas razoáveis dos titulares [54].

---

51 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

52 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

53 GELLERT, Raphael. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. **European Data Protection Law Review**, n. 2, pp. 212-217, Berlim, 2017.

54 GELLERT, Raphael. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. **European Data Protection Law Review**, n. 2, pp. 212-217, Berlim, 2017.

Como exemplo para o enquadramento de atividades no quarto critério, o guia orientativo refere a guarda de formulários médicos de pacientes por hospitais ou dados de investigação criminal de um indivíduo guardados pela autoridade investigadora. Além das previsões do GDPR, alguns tipos de dados podem potencialmente aumentar o risco às liberdades e direitos dos titulares justamente por estarem relacionados a atividades privadas. Nesse sentido, esse critério pode incluir dados como documentos pessoais, e-mails, diários etc.[55].

A partir do supracitado critério, pode-se inferir que operações realizadas com conteúdo presente nas redes sociais, como registros de momentos pessoais dos usuários, como nascimento de um filho, por exemplo, poderiam estar englobadas pelo quarto critério. No entanto, a análise de alto risco da operação deve ser realizada considerando o contexto da operação, como a eventual publicização anterior do dado pelo próprio titular. Assim, nesse caso, seria relevante para a avaliação de eventual operação de tratamento realizada com os dados em questão o fato de os titulares já terem tornado públicas as informações anteriormente à operação de tratamento.

Além dos pontos acima elencados pelo *Article 29 Working Party* como critérios para identificar operações de alto risco, o guia orientativo também explica e esclarece alguns outros critérios derivados daqueles previstos no próprio artigo 35 do GDPR[56].

Esse é o caso do quinto critério, que envolve o tratamento de dados em larga escala. Nesse ponto, como o GDPR não define o que seria tratamento de dados em larga escala, o guia orientativo recomenda que alguns fatores sejam considerados para determinar se um tratamento de dados é realizado em larga escala, tais quais: i) o número de titulares de dados atingidos pelo tratamento, tanto como um número absoluto como em relação à proporção da população; ii) o volume dos dados a ser processado; iii) a duração da atividade de tratamento; e iv) a extensão geográfica da atividade de tratamento[57].

---

55 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

56 GELLERT, Raphael. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. **European Data Protection Law Review**, n. 2, pp. 212-217, Berlim, 2017.

57 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

Como a definição de tratamento em larga escala é relevante tanto para identificar o critério previsto pelo guia orientativo quanto para a identificação da hipótese de necessidade de elaboração de DPIA prevista pelo próprio GDPR, tal conceito é analisado de forma mais detalhada no próximo subcapítulo, a partir das definições sobre o conceito presentes em outro documento expedido pelo *Article 29 Working Party*.

Adicionalmente, o *Article 29 Working party* também inclui novos critérios, diferentes daqueles previstos no texto legal do GDPR, deixando claro que a análise desses critérios permanece contextualizada[58].

Isso acontece no sexto critério identificado pelo guia orientativo, que versa sobre a combinação de bases de dados, como uma operação de tratamento que surge a partir de outas duas ou mais operações de tratamento de dados realizadas para diferentes finalidades e/ou por diferentes controladores, de modo que o titular pode não esperar a operação de tratamento em questão. Ou seja, o cruzamento de dados coletados em diferentes operações de tratamento para diferentes finalidades para a inferência de novas informações ou como subsídio para a realização de nova atividade pode estar enquadrado no critério em questão[59].

O sétimo critério referido no documento é o tratamento de dados relacionados a indivíduos vulneráveis. Tal atividade de tratamento é considerada um critério em razão do maior desequilíbrio de poder entre o titular, que é uma pessoa vulnerável, e o controlador dos dados, de modo que esses indivíduos podem não ser capazes de exercer seus direitos, consentir ou se opor ao tratamento realizado pelo controlador. Como exemplo de indivíduos vulneráveis, foi apontado crianças, empregados e seguimentos mais vulneráveis da sociedade (como pessoas com doenças mentais, pessoas idosas ou em qualquer situação na qual possa se identificar um desequilíbrio entre a posição do controlador e do titular)[60].

---

58 GELLERT, Raphael. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. **European Data Protection Law Review**, n. 2, pp. 212-217, Berlim, 2017.

59 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

60 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

O oitavo critério estipulado pelo *Article 29 Working Party* refere-se a operações que utilizem ou apliquem, de forma inovadora, novas soluções tecnológicas ou organizacionais. Quanto a esse critério, há de se considerar que o próprio artigo 35 (1) do GDPR aponta que o uso de novas tecnologias por uma operação de tratamento de dados pode desencadear a necessidade de elaboração de um DPIA. Isso porque, as consequências pessoais ou sociais do desenvolvimento de novas tecnologias podem ser desconhecidas. Assim, a elaboração de um DPIA pode ajudar o controlador a identificar e mitigar eventuais riscos atrelados ao uso desses tipos de tecnologia[61].

Como exemplo de operação que estaria enquadrada no critério em questão, o *Article 29 Working Party* aponta a combinação de dados de biometria e reconhecimento facial de indivíduos para melhorar o controle de acesso físico a ambientes[62].

E, considerando que tal critério compreende não só o uso de novas soluções tecnológicas, ou seja, quando a tecnologia utilizada é, em si, inovadora, mas também o caso de uso de novas soluções organizacionais, é possível se concluir que o uso de uma tecnologia, mesmo que não necessariamente nova, por um agente de tratamento como nova solução organizacional pode estar, também, enquadrado no critério em questão.

Por fim, como nono critério, o guia orientativo apresenta o caso de operações de tratamento que, por si mesmas, impeçam os titulares de exercer um direito ou usar um serviço ou contrato, o que inclui operações cuja finalidade seja permitir, modificar ou recusar o acesso dos titulares dos dados a serviços ou contratos. Como exemplo, foi referida a análise realizada por instituições financeiras para fins de decisão sobre a concessão de empréstimos aos clientes[63].

---

61 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

62 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

63 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

O guia orientativo estabeleceu um sistema flexível e contextualizado a partir dos nove critérios gerais mencionados ao longo do documento. Como regra geral, estabeleceu que se em uma operação de processamento de dados são identificados pelo menos dois dos nove critérios, pode-se assumir que se trata de uma operação de alto risco, regra que, no entanto, depende de uma avaliação contextualizada, visto que, em alguns casos, o controlador pode entender que apenas um critério seria suficiente para indicar o alto risco de uma operação[64].

A partir disso, verifica-se que, a despeito da tentativa de estipular uma metodologia mais objetiva para a aplicação dos critérios como identificadores de casos sujeitos à elaboração de DPIA, inevitavelmente remanesce certo grau de subjetividade na análise, vez que é necessária uma análise contextualizada e circunstancial de cada operação, podendo, em alguns casos, ser identificado um alto risco em operações que contemplem apenas um critério.

A partir disso, percebe-se uma das dificuldades ligadas ao DPIA e à metodologia baseada em risco. Isso porque, considerando que o DPIA deve ser um meio de possibilitar aos controladores maior flexibilidade e discrição a suas operações, prever uma lista exaustiva de operações de alto risco significaria ir contra a própria lógica do DPIA e a metodologia de risco prevista no GDPR[65].

De forma geral, o *Article 29 Working Party* entende que quanto mais critérios forem identificados nas operações de tratamento, mais essas operações estarão sujeitas a apresentar elevado risco e, consequentemente, demandar a elaboração de DPIA.

Ainda, além de apresentar os nove critérios a serem considerados para a identificação de operações suscetíveis de causar elevados riscos aos titulares, como complemento didático, o *Article 29 Working Party* elaborou um quadro com exemplos práticos de processamento de dados e identificação de critérios respectivos, a fim de demonstrar como pode ser feita a análise pelo controlador para decisão sobre a elaboração de um DPIA[66].

---

64 GELLERT, Raphael. EDPB Opinion on the Draft Lists of Competent Supervisory Authorities regarding the Processing Operations Subject to DPIAs. **European Data Protection Law Review**, n. 4, pp. 500-504, Berlim, 2018.

65 GELLERT, Raphael. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. **European Data Protection Law Review**, n. 2, pp. 212-217, Berlim, 2017.

66 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

Para fins de ilustração da proposta didática presente no guia orientativo, entende-se pertinente a referência a uma versão resumida do quadro constante no documento, conforme o Quadro 1, a seguir:

Quadro 1: Exemplos de análise prática de exigência de DPIA

Exemplos de tratamento	**Critérios pertinentes possíveis**	**Exige-se a realização de um DPIA?**
Controle, por uma empresa, das atividades dos seus empregados, incluindo controle dos computadores, atividades na internet etc.	- Controle sistemático (terceiro critério) - Dados de titulares vulneráveis (sétimo critério)	Sim
Coleta de dados públicos das redes sociais para elaboração de perfis	- Avaliação ou classificação. (primeiro critério) - Dados tratados em grande escala. (quinto critério) - Combinar conjuntos de dados. (sexto critério) - Dados sensíveis ou dados de natureza altamente pessoal (quarto critério)	Sim
Uma revista online que utiliza e-mails para enviar conteúdo diariamente para seus inscritos	- Processamento de dados em larga escala (quinto critério)	Não

Fonte: elaborado pela autora (2022)[67].

Ainda, é referido no guia orientativo que uma operação de tratamento pode corresponder a um dos casos referidos no quadro como sujeito à elaboração de DPIA e, ainda assim, o controlador entender que não se trata de operação suscetível de apresentar elevados riscos aos titulares. Nesses casos, o controlador deve documentar as razões pelas quais não elaborou um DPIA, além de incluir a opinião do *data protection officer*[68] acerca da situação[69].

---

[67] Quadro resumido e complementado pela autora a partir de quadro previsto no documento Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022).

[68] Figura presente no GDPR que é equivalente ao encarregado de dados no contexto da lei brasileira de proteção de dados.

[69] UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

Se analisados os exemplos trazidos pelo *Article 29 Working Party* ao longo do guia orientativo, mostra-se realmente lógico que a combinação de, pelo menos, dois critérios em uma operação de tratamento indique potencial elevado de risco aos direitos e liberdades dos titulares, principalmente se analisados comparativamente aos exemplos trazidos pelo próprio texto legal do GDPR.

Em análise mais atenta, percebe-se que os cinco primeiros critérios listados no guia orientativo são derivações mais detalhadas das hipóteses constantes no parágrafo terceiro do artigo 35 do GDPR.

O primeiro exemplo referido no parágrafo terceiro do Artigo 35 envolve operações com sistemática e extensiva avaliação de aspectos pessoais relacionados aos titulares que sejam baseadas em processos automatizados, incluindo *profiling*[70]*.* Por sua vez, os dois primeiros critérios apresentados pelo *Article 29 Working Party* no guia orientativo consistem em: i) operações de avaliação ou classificação de pessoas naturais, incluindo o *profiling* e ii) decisões automatizadas que produzam efeitos jurídicos ao titular ou o afetem de modo similar[71]. Ou seja, a combinação do primeiro e do segundo critério estipulados no guia orientativo constitui, de forma mais detalhada e concreta, o primeiro exemplo constante no texto do GDPR.

Situação semelhante se verifica em relação aos terceiro e quinto critérios previstos no guia orientativo, que, juntos, correspondem ao terceiro exemplo do artigo 35, parágrafo terceiro, do GDPR. O terceiro critério aborda o monitoramento sistemático de áreas publicamente acessíveis e o quinto critério se refere a dados tratados em larga escala[72]. Por sua vez, o terceiro exemplo do texto legal do GDPR consiste em operações que envolvam o monitoramento sistemático em área publicamente acessível (terceiro critério) em larga escala (quinto critério)[73].

---

70 Artigo 35, 3, “a” (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022).

71 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

72 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

73 Artigo 35, 3, “c” (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022).

Ainda, o quarto critério, que contempla o tratamento de dados sensíveis ou de natureza altamente pessoal, combinado com o quinto critério, que se refere ao tratamento em larga escala[74], corresponde ao segundo exemplo do GDPR, que trata de operações em larga escala de dados sensíveis ou condenações penais e infrações[75].

Ou seja, nesses casos, se aplicado o método de combinação de, pelo menos, dois critérios em uma atividade de tratamento de dados para que se identifique a necessidade de elaboração de DPIA, chega-se a atividades contempladas pelas hipóteses de tratamento que demandam a elaboração de relatório de impacto previstas no próprio texto legal do GDPR.

Claro que, além dos critérios derivados das hipóteses presentes no próprio GDRP, abordados de maneira mais detalhada e específica, o *Article 29 Working Party* apresentou novos critérios a serem, também, considerados para fins de identificação de operações de tratamento que demandam a elaboração de relatório de impacto.

No entanto, essa análise de equivalência dos critérios em relação às hipóteses previstas no dispositivo legal serve como uma espécie de validação da metodologia proposta no guia orientativo, demonstrando que o método elaborado é realmente efetivo e compatível com as disposições do GDPR.

Ainda, além de apresentar critérios para identificação de hipóteses nas quais seria necessária a elaboração de DPIA, o *Article 29 Working Party*, no guia orientativo objeto de análise do presente subcapítulo, também se propôs a elaborar critérios para identificar hipóteses nas quais não seria necessária a elaboração de relatório de impacto[76].

---

74 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

75 Artigo 35, 3, "b" (UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022).

76 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

Segundo o órgão consultivo, a elaboração de DPIA não seria necessária no caso de operações de tratamento que não estivessem sujeitas a resultar em elevado risco aos direitos e liberdades dos titulares[77].

Os exemplos apresentados pelo *Article 29 Working Party* para tais situações foram: i) operações cuja natureza, escopo e finalidade do tratamento de dados pessoais são muito similares a operações em relação às quais já tenha sido elaborado um DPIA, hipótese na qual poder-se-ia utilizar os resultados do DPIA elaborado para a atividade similar respectiva; ii) quando a operação tiver sido verificada por uma autoridade de supervisão antes de maio de 2018 e cujas condições não tenham sido alteradas desde então; iii) quando uma operação de tratamento que estiver enquadrada na base legal do cumprimento de obrigação legal ou para fins de exercício do interesse público ou de autoridade pública em que está investido o agente de tratamento tiver fundamento jurídico no direito da União Europeia ou de um Estado-Membro e em relação à qual um relatório de impacto já tenha sido elaborado como parte da adoção desse fundamento; e iv) quando o tratamento de dados em questão estiver abarcado pela lista de atividades em relação às quais a elaboração de DPIA é opcional, a ser elaborada pelas autoridades nacionais de proteção de dados[78].

As hipóteses referidas no documento como tipos de atividade de tratamento que não demandariam a elaboração de DPIA podem ser resumidas a atividades de tratamento que, de alguma forma, já estejam contempladas em um DPIA já elaborado, tenham sido previamente validadas por uma autoridade nacional ou, ainda, ocorram para fins de cumprimento de obrigação legal ou atendimento a interesse público quando o agente de tratamento é órgão estatal.

Ou seja, com exceção da hipótese referente ao agente público, as demais hipóteses não são tipos de atividades que, em razão da sua natureza ou características pré-definidas, estariam dispensadas da elaboração de DPIA, mas sim atividades que já estariam previamente contempladas em relatório de impacto ou que,

---

77 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

78 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

a partir de uma análise individual e específica, tenham sido autorizadas pela autoridade nacional.

Diferente da lista de critérios para identificação das hipóteses que demandariam a elaboração de DPIA, a lista de hipóteses de atividades que estariam liberadas da elaboração do relatório de impacto não fornece critérios muito concretos e objetivos que possam auxiliar a prática dos agentes de tratamento.

Conclusivamente, a partir da análise do "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679",* elaborado pelo *Article 29 Working Party*, verifica-se que o documento tornou mais objetiva a análise da necessidade de elaboração de DPIA pelos agentes de tratamento, aumentando o grau de segurança jurídica no que se refere ao tema.

No entanto, em razão das inúmeras possibilidades de atividades envolvendo o processamento de dados atualmente, inevitável grau de subjetividade ainda permeia as orientações expedidas pelo órgão consultivo, de modo que os critérios definidos e os exemplos apresentados não constituem um rol taxativo de hipóteses que demandam a elaboração de DPIA e, consequentemente, não podem ser tratados como se o fossem.

2.2.3 Definições sobre tratamento em larga escala e monitoramento sistemático e regular presentes no documento *"Guidelines on Data Protection Officers"*

Considerando que tanto nos exemplos de atividades de tratamento de dados que demandam a elaboração de DPIA previstos no texto legal do GDPR (artigo 35, parágrafo terceiro, "b" e "c"), quanto nos critérios definidos no guia orientativo do *Article 29 Working Party* sobre DPIA (critérios 3 e 5), os conceitos de tratamento em larga escala e monitoramento sistemático aparecem não apenas de forma secundária, mas como o próprio cerne das hipóteses que exigiriam a elaboração de DPIA, para que seja possível, na prática, identificar as atividades que estariam enquadradas em tais situações, é necessário compreender o que seria tratamento em larga escala e monitoramento sistemático.

Diante da lacuna de definição sobre tratamento em larga escala e monitoramento sistemático pelo texto legal do GDPR, além da definição ventilada pelo

considerando 91 do GDPR, já abordada no subcapítulo anterior, busca-se subsídios para a compreensão dos conceitos no guia orientativo do *Article 29 Working Party* denominado "*Guidelines on Data Protecion Officers"*[79].

O Guia Orientativo expõe que não é possível definir um número preciso de dados tratados ou de titulares afetados pela atividade de tratamento para que esta seja considerada de larga escala. No entanto, o *Article 29 Working Party* recomenda alguns fatores a serem considerados para essa análise, sendo: i) o número de titulares afetados pelo tratamento, tanto como número absoluto ou referente à proporção de uma população; ii) o volume de dados ou as categorias de dados tratados; iii) a duração da atividade de tratamento de dados; e iv) a extensão geográfica da operação de tratamento de dados[80].

Diferente do que se verifica no *Guidelines on DPIA* abordado anteriormente, no qual há a definição de uma metodologia para a identificação das hipóteses que demandariam a elaboração de relatório de impacto (a combinação de, pelo menos, dois dos critérios elencados), no *Guidelines on DPO* não há qualquer definição mais objetiva sobre eventual combinação dos fatores apontados para fins de identificação de tratamento em larga escala. Da mesma forma, também não foram propostos critérios mais precisos sobre como considerar os fatores apontados, de modo que a análise das atividades de tratamento de dados, na prática, para fins de seu enquadramento como atividades de tratamento de larga escala deverá ser subjetiva e realizada caso a caso[81].

No entanto, a fim de fornecer mais subsídios para a classificação de operações de tratamento em larga escala, o guia orientativo apresenta alguns exemplos de tratamento que seriam considerados de larga escala, sendo eles: i) tratamento de dados de pacientes por hospitais em suas atividades rotineiras; ii) tratamento de dados de deslocamento de indivíduos que utilizam sistema de transporte público; iii) processamento de dados de geolocalização em tempo real de clientes de uma rede internacional de fast food para fins estatísticos por um agente de tratamento

---

79 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

80 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

81 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

especializado em fornecer esse tipo de serviço; iv) processamento de dados pessoais no contexto de administração regular de negócio por bancos ou seguradoras; v) tratamento de dados pessoais para fins de publicidade dirigida com base em análise comportamental dos titulares; e vi) processamento de dados por provedores de internet ou telefone[82].

Em análise aos exemplos apresentados pelo *Article 29 Working Party* acima referidos, é possível concluir que, em sua maioria, estão presentes pelo menos dois dos fatores previamente definidos pelo guia orientativo. Por exemplo, “tratamento de dados pessoais para fins de publicidade dirigida” contempla tanto uma quantidade elevada de titulares afetados, como número elevado de dados de cada um dos titulares, além de extensa duração da atividade de tratamento e, eventualmente, também uma ampla extensão geográfica do tratamento, uma vez que essas atividades de análise de dados para fins de direcionamento de publicidade com base nas características comportamentais dos titulares são muito comuns em ferramentas digitais que contêm dados de pessoas do mundo inteiro.

Ainda, o documento também refere alguns exemplos de atividade que não estariam enquadradas como tratamento de larga escala. São elas: i) tratamento de dados de pacientes por um médico individual e ii) tratamento de dados sobre condenações penais por um advogado[83].

Provavelmente os exemplos foram escolhidos porque o tratamento de dados de clientes realizado individualmente por um profissional liberal, como regra, não envolve um número muito expressivo de dados como acontece quando o tratamento é realizado por grandes empresas ou instituições, por exemplo. Diante disso, pode-se pensar que para que o volume de dados ou titulares afetados por um tratamento seja considerado elevado para fins de classificação da atividade como tratamento em larga escala, ele deve contemplar um número realmente expressivo de titulares e dados. No entanto, essa análise deve ser realizada considerando todo o contexto da operação de tratamento, inclusive, eventualmente, a tecnologia utilizada para o processamento dos dados em questão.

---

82 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

83 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

Por fim, o guia orientativo também aborda a conceituação de monitoramento sistemático e regular de dados, que também não é definida no texto legal do GDPR, sendo que a menção ao tema se restringe à abordagem do conceito de monitoramento do comportamento de titulares de dados mencionado no considerando número 24 do GDPR, que inclui as formas de rastreamento e perfilamento na internet. No entanto, refere-se no documento que a noção de monitoramento não é restrita ao ambiente virtual e o rastreamento online deve ser considerado apenas um exemplo de monitoramento do comportamento dos titulares de dados[84].

Nesse sentido, o *Article 29 Working Party* interpreta "regular" como tratamentos enquadrados em, pelo menos, uma das seguintes situações: i) ocorrência em determinados intervalos em um determinado período; ii) recorrência ou repetição em momentos fixos; iii) de forma constante ou periódica[85].

Já, "sistemático" é interpretado como operações de tratamento que se encaixam em pelo menos uma das seguintes situações: i) ocorrência de acordo com um sistema; ii) de maneira pré-arranjada, organizada ou metódica; iii) parte de um plano geral de coleta de dados; iv) realizados como parte de uma estratégia[86].

Como exemplos de atividades que podem ser consideradas monitoramento regular e sistemático de titulares, o guia orientativo aponta: i) operação de telecomunicação; ii) redirecionamento de e-mails; iii) atividades de marketing dirigidas por análise de dados; iv) perfilamento para fins de avaliação de risco; v) monitoramento de localização por dispositivos móveis; vi) monitoramento de saúde por dispositivos; entre outros[87].

A partir da análise do guia orientativo, verifica-se que a conceituação de "monitoramento sistemático e regular" e "tratamento em larga escala" é importante para fins de fornecimento de subsídios aos agentes de tratamento de dados para a identificação, nas atividades práticas, das operações de tratamento que estariam

---

84 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

85 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

86 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

87 UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

enquadradas nos exemplos apresentados no texto legal do GDPR e critérios definidos pelo *Article 29 Working Party no Guidelines on DPIA* e que, portanto, demandariam a elaboração de relatório de impacto.

2.3 HISTÓRICO DE SANÇÕES ADMINISTRATIVAS RELACIONADAS À FALTA DE ELABORAÇÃO DE DPIA

De forma a concluir a primeira parte do desenvolvimento do presente estudo, para verificar, na prática, como tem sido exigida a elaboração de relatórios de impacto no âmbito da União Europeia, o presente subcapítulo se propõe a analisar o histórico de sanções impostas por autoridades nacionais de dados nos países da União Europeia no que se refere à falta de elaboração de DPIA quando necessário pelos agentes de tratamento.

Como fonte de pesquisa, foi utilizada a base de dados do *GDPR Enforcement Tracker*[88], ferramenta online que reúne um apanhado das multas e penalidades impostas por autoridades de dados no âmbito da União Europeia em relação às obrigações constantes no GDPR. No entanto, faz-se a ressalva de que como nem todas as sanções são publicizadas, a lista pode não contemplar absolutamente todas as sanções já impostas no âmbito da União Europeia.

Como filtro para a pesquisa, foram selecionadas as sanções que têm como fundamento a violação do artigo 35 do GDPR, tendo em vista que a previsão de obrigatoriedade para a elaboração de relatório de impacto se encontra no referido artigo legal.

Dentre os 23 resultados apresentados para sanções envolvendo violação do artigo 35 do GDPR, foram identificadas 11 situações nas quais as motivações para a imposição das sanções envolveram, entre outras violações ao GDPR, a ausência de elaboração de DPIA quando se fazia necessário para a atividade em questão[89].

As sanções envolvendo a elaboração de DPIA foram impostas pelas autoridades de proteção de dados dos seguintes países: Espanha, Portugal, Itália, Noruega, Lituânia e Finlândia. Na maioria das situações, além da falta de elaboração

---

88 GDPR Enforcement Tracker. [**Homepage**]. [*S.l.*], 2022. Disponível em: https://www.enforcementtracker.com/. Acesso em: 22 abr. 2022.

89 GDPR Enforcement Tracker. [**Homepage**]. [*S.l.]*, 2022. Disponível em: https://www.enforcementtracker.com/. Acesso em: 22 abr. 2022.

de DPIA pelo controlador, outras violações ao GDPR foram identificadas nas atividades de tratamento como fundamento para a imposição das sanções pelas autoridades de dados[90].

Ao analisar as atividades de tratamento de dados objeto das sanções, é possível identificar a ocorrência dos seguintes critérios previstos no *Guidelines on DPIA* pelo *Article 29 Working Party* como indicativos de operações suscetíveis de resultar em elevado risco aos titulares e que, portanto, demandariam a elaboração de DPIA: i) operações envolvendo dados sensíveis; ii) monitoramento sistemático; iii) operações de avaliação ou classificação; iv) tratamento de dados em larga escala; v) dados de titulares vulneráveis; e vi) uso ou aplicação de soluções tecnológicas inovadoras. Além disso, algumas das operações poderiam estar enquadradas nas hipóteses previstas no artigo 35, parágrafo terceiro, "a" e "b", do GDPR, sendo elas operações que envolvem sistemática e extensiva avaliação de aspectos pessoais relacionados a pessoas naturais que sejam baseadas em processos automatizados, incluindo *profiling* e operações de tratamento em larga escala de dados sensíveis[91].

A fim de ilustrar a análise realizada para fins de identificação dos critérios presentes nas atividades que foram objeto de sanções e em relação às quais as respectivas autoridades de dados competentes entenderam que a elaboração de DPIA era necessária, utiliza-se dois exemplos de sanções identificadas a partir da pesquisa realizada.

A empresa "Serviços Logísticos Martorell Siglo XXI, S.L." foi multada pela Autoridade de Dados da Espanha (AEPD) em razão da instalação, pela empresa, de cinco terminais com controle por biometria para registo dos horários de expediente realizados por seus empregados. Ao realizar a atividade de dados, a autoridade considerou que a empresa falhou ao não elaborar um DPIA[92].

---

90 GDPR Enforcement Tracker. [**Homepage**]. [*S.l.*], 2022. Disponível em: https://www.enforcementtracker.com/. Acesso em: 22 abr. 2022.

91 GDPR Enforcement Tracker. [**Homepage**]. [*S.l.*], 2022. Disponível em: https://www.enforcementtracker.com/. Acesso em: 22 abr. 2022.

92 "*Authority: Spanish Data Protection Authority (aepd). Sector: Industry and Commerce. Summary: The Spanish DPA (AEPD) has imposed a fine on SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.I. The company had installed five terminals with a fingerprint control system to record its employees' working hours. In doing so, the company had failed to conduct a data protection impact assessment. The AEPD found a violation of Art. 35 GDPR for this reason. The original fine of EUR 20,000 was reduced to EUR 16,000 due to voluntary payment. GDPR Enforcement Tracker*" (GDPR Enforcement Tracker. [**Homepage**]. [*S.l.*], 2022. Disponível em: https://www.enforcementtracker.com/. Acesso em: 22 abr. 2022).

No caso acima relatado, por exemplo, é possível identificar a presença dos seguintes critérios previstos pelo *Article 29 Working Party* como indicativos da necessidade de elaboração de DPIA: i) tratamento de dados sensíveis (dados biométricos); ii) monitoramento regular e sistemático; iii) dados de titulares vulneráveis (empregados subordinados ao controlador); iv) uso ou aplicação de soluções tecnológicas inovadoras (não pela tecnologia, em si, ser considerada inovadora, mas em razão de seu uso pela empresa ser novo).

O outro exemplo se refere à empresa de serviços de delivery de comida "Deliveroo Italy s.r.l.", que foi multada pela Autoridade de Dados Nacional da Itália por realizar o tratamento ilícito de dados de 8 mil motoristas. Foram apontados como violações ao GDPR presentes na operação de tratamento a falta de transparência dos algoritmos utilizados, falta de informação aos titulares sobre o tratamento em questão, tratamento excessivo de dados para a finalidade pretendida e falta de elaboração de DPIA[93].

Nessa hipótese, pode-se concluir que a necessidade de elaboração de DPIA decorre da combinação dos seguintes critérios previstos pelo *Article 29 Working Party*: i) monitoramento sistemático e regular de dados; ii) tratamento de dados em larga escala; e iii) uso de aplicação ou solução tecnológica inovadora.

A partir da análise do histórico de sanções pelas autoridades nacionais de proteção de dados na União Europeia envolvendo a falha dos controladores na elaboração de DPIA, conclui-se que as hipóteses que as autoridades identificaram

---

93 "*Authority: Italian Data Protection Authority (Garante). Sector: Industry and Commerce.*
Summary: The Italian DPA (Garante) has fined food delivery service Deliveroo Italy s.r.l. EUR 2,500,000 for unlawfully processing the personal data of approximately 8000 drivers. Garante's investigation revealed numerous and serious data protection violations. The violations included a lack of transparency in the algorithms used to manage drivers, both when assigning jobs and when booking work shifts. Deliveroo had used a centralized system for driver management through which it then processed and managed the assignment of orders as well as the booking of work shifts. However, Garante notes that the controller did not adequately inform the drivers about the functioning of the system they had installed on their smartphones and did not ensure the accuracy and correctness of the results of the algorithmic systems used to evaluate the drivers. In addition, Garante found that Deliveroo carried out a meticulous control of the drivers' work performance - through the continuous geolocation of their device, which went far beyond what was necessary to assign the order (e.g., recording the position every 12 seconds) - and through the storage of a large amount of personal data collected during the execution of the orders, including communication with customer service. In this context, the storage period of the various data had not been defined in a manner appropriate to the purpose. Instead, the controller had defined a flat storage period of six years. Furthermore, the Garante found that the controller had not implemented adequate technical and organizational measures to ensure adequate security of the processing. Deliveroo Italy had also not conducted a data protection impact assessment, although this would have been necessary due to the risk posed to the drivers" (GDPR Enforcement Tracker. [**Homepage**]. [*S.l.*], 2022. Disponível em: https://www.enforcementtracker.com/. Acesso em: 22 abr. 2022).

como sendo necessária a elaboração do relatório de impacto são condizentes com os critérios definidos pelo *Article 29 Working Party* para a identificação de operações de tratamento que, por implicarem elevados riscos aos titulares de dados, demandariam a elaboração de DPIA.

Assim, percebe-se que os critérios desenvolvidos no *Guidelines* e as hipóteses previstas no artigo 35 do GDPR, objeto de análise nos tópicos anteriores do presente trabalho, são utilizados na prática da fiscalização das autoridades nacionais para a identificação de atividades de tratamento de dados que demandam a elaboração de DPIA e têm sido utilizados para nortear as autoridades de tratamento quando da imposição de sanções pela inobservância das obrigações previstas na legislação de proteção de dados da União Europeia.

3 O RELATÓRIO DE IMPACTO NO CONTEXTO BRASILEIRO

Ultrapassada a análise da regulamentação europeia acerca das hipóteses de exigência do relatório de impacto, o presente capítulo se propõe a analisar o desenvolvimento da temática no Brasil.

Para isso, enfrenta-se, em um primeiro plano, a regulamentação do tema pela Lei Geral de Proteção de Dados (LGPD), e, em um segundo plano, subsídios interpretativos para a matéria e atuação da ANPD até o momento da escrita do presente trabalho.

3.1 A LGPD NA REGULAMENTAÇÃO DO TEMA

O Relatório de Impacto à Proteção de Dados brasileiro é definido como a documentação do controlador[94] destinada a descrever os processos de tratamento de dados que podem causar riscos às liberdades civis e direitos fundamentais dos titulares, bem como a indicar medidas, salvaguardas e mecanismos de mitigação desses riscos[95].

A partir da definição do documento prevista na LGPD, é possível segmentar o Relatório de Impacto em três partes: i) uma documentação do controlador, ou seja, o Relatório de Impacto deve ser apresentado pelo Controlador como documento formal que contemple os critérios necessários para sua estruturação; ii) descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades e direitos dos titulares, sendo este um dos pontos que o documento deve contemplar; e iii) previsão de medidas e salvaguardas para mitigação dos riscos identificados, o que indica que, além de identificar os riscos que as operações de tratamento apresentam aos titulares, o Relatório de Impacto deve, também, prever medidas para a mitigação de tais riscos[96].

---

94 A LGPD conceitua o controlador como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões relevantes sobre o tratamento de dados pessoais (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

95 Art. 5º, XVII (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

96 GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados: Uma breve análise da sua definição e papel na LGPD. **Revista do Advogado**, São Paulo, ano 39, n. 144, pp. 174-183, nov. 2019.

O documento se insere em um contexto de ações de governança em privacidade do controlador, viabilizando o cumprimento de inúmeros princípios da LGPD. Assim, o relatório de impacto deve ser compreendido não só como mais uma das obrigações impostas pela LGPD aos agentes de tratamento, mas também como um instrumento útil à avalição de impacto das atividades de tratamento de dados, o que contribui para uma cultura de proteção de dados corporativa[97].

No entanto, percebe-se que no contexto brasileiro de desenvolvimento da matéria, há, ainda, uma compreensão equivocada sobre o que é o Relatório de Impacto e quais são as suas funções.

Por vezes, há uma confusão entre o Relatório de Impacto e o relatório de diagnóstico, que serve para medir o nível de adequação de um agente de tratamento de dados à LGPD, ou o teste do legítimo interesse, que serve para analisar se uma operação pode ser legitimamente enquadrada na base legal do legítimo interesse. Importante ter claro que, diferente desses outros documentos, o Relatório de Impacto trata-se de documento destinado à análise de uma operação individual, ou conjunto de operações que guardam afinidades entre si, para fins de mapeamento de riscos que apresentam aos titulares dos dados e indicação de medidas e mecanismos para prevenir e mitigar esses riscos[98].

Já no que se refere à elaboração do documento, verifica-se que, de acordo com a definição do documento prevista na LGPD, a sua necessidade está relacionada a operações de tratamento de dados que são consideradas de alto risco por uma autoridade. Ora, caso a regra fosse a elaboração do documento quando a operação de tratamento implica qualquer risco ao titular, seria necessário elaborar Relatório de Impacto para toda e qualquer operação de tratamento de dados, vez que todas as atividades de tratamento de dados pessoais apresentam, inerentemente, certo risco aos titulares[99].

---

97 MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019, p. 126 e 130.

98 GOMES, Maria Cecília Oliveira. LGPD: Desafios da regulamentação do relatório de impacto. **Jota**, [*S.l.*], 11 fev. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. Acesso em: 22 abr. 2022.

99 GOMES, Maria Cecília Oliveira. LGPD: Desafios da regulamentação do relatório de impacto. **Jota**, [*S.l.*], 11 fev. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. Acesso em: 22 abr. 2022.

Ocorre que, diferentemente do GDPR, a LGPD não esclarece quais seriam as hipóteses nas quais seria necessária a elaboração do Relatório de Impacto, de modo que são breves e limitadas as referências à exigibilidade do documento ao longo do texto legal.

Um dos poucos artigos que apresentam um indicativo sobre possível exigência do documento é o artigo 38 da LGPD, no qual está prevista a possibilidade de exigência do documento pela Autoridade Nacional de Proteção de Dados (ANPD):

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados[100].

Verifica-se que, de acordo com o dispositivo legal, a regulamentação mais específica do tema é de responsabilidade da própria ANPD. No entanto, independentemente dessa futura regulamentação pela Autoridade Nacional, a partir da redação do dispositivo legal, é possível identificar a sinalização de possível exigibilidade do documento no caso de tratamento de dados sensíveis[101].

Outro indicativo de hipóteses nas quais poderia ser exigida a elaboração do Relatório de Dados pelo controlador encontra-se no artigo 10, parágrafo 3º, da LGPD[102], que indica que a ANPD pode solicitar o Relatório de Impacto ao controlador quando presente o legítimo interesse como base legal, hipótese que, contudo, não chegou a ser detalhada no texto legal[103].

---

[100] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022.

[101] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019, p. 311.

[102] "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: [...] § 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 n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

[103] HAYDUK, Gabriel. Requisitos do Relatório de Impacto à Proteção de Dados Pessoais. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, p. 569-585, p. 570.

Ainda, no artigo 4º, parágrafo 3º da LGPD, também há a referência de possível exigência de Relatório de Impacto pela ANPD nos casos que estariam enquadrados na previsão de exceção de aplicação da LGPD prevista no inciso III do mesmo artigo, que, por sua vez, se refere a tratamentos de dados realizados pelo poder público para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação penal[104]. Ou seja, diante dos riscos decorrentes do tratamento de dados nessas hipóteses pela administração pública, ainda que a essas operações de tratamento de dados não sejam aplicáveis as disposições da LGPD, é coerente que a ANPD possa solicitar aos responsáveis relatórios de impacto[105].

Por fim, o artigo legal que, juntamente com o art. 5º, XVII da LGPD, corrobora a hipótese de que a legislação brasileira, nos moldes do que se verifica no GDPR, optou por uma metodologia baseada em risco para fins de exigência do Relatório de Impacto, é o artigo 55-J, inciso XIII da LGPD, incluído pela Lei nº 13.853/2019, que cria a Autoridade Nacional de Proteção de Dados e dá outras providências:

> Art. 55-J. Compete à ANPD:
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei[106].

No entanto, apesar dos indícios de opção da LGPD pela metodologia de risco, verifica-se que, ao discorrer sobre o Relatório de Impacto, a Lei parece silenciar quanto ao processo anterior à sua efetiva elaboração, que seria justamente a identificação das operações de tratamento de dados que demandariam a elaboração do Relatório de Impacto[107].

Ocorre que tal cenário de incertezas pode levar a uma banalização do documento e excessiva oneração dos agentes de tratamento, que, muitas vezes,

---

[104] Art. 4º, III e § 3º (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

[105] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019, p. 87.

[106] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

[107] TIMM, Luciano; CAOVILLA, Renato; STURARI, Mateus. O Relatório de Impacto na LGPD: Sentido e Limites Dentro da Regulação Econômica. *In*: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coords.). **Proteção de Dados:** Temas Controvertidos. Indaiatuba: Editora Foco, 2021, pp. 362-384.

acabam elaborando o Relatório de Impacto em toda hipótese que pode, minimamente, implicar alguma exigência de sua elaboração, situação negativa que, além de gerar excessiva onerosidade aos agentes de tratamento, acaba por banalizar o documento, que passa a ser encarado como mero cumprimento burocrático de obrigação da LGPD, quando na verdade deveria servir para garantir uma análise prévia dos riscos das operações de tratamento a fim de resguardar direitos e interesses dos titulares[108].

Diante da ausência de disposição legal específica e clara sobre as hipóteses de exigência do Relatório de Impacto, busca-se a dedução de alguns possíveis balizadores a partir de uma análise sistemática da LGPD.

A partir dessa análise sistemática da Lei, é possível identificar algumas hipóteses nas quais a ANPD poderia exigir a elaboração do Relatório de Impacto à Proteção de Dados, que seriam: i) quando o tratamento envolver dados sensíveis; ii) quando o tratamento for fundamentado na base legal do legítimo interesse e iii) quando o tratamento de dados apresentar alto risco à garantia dos princípios gerais de proteção de dados previstos na Lei.

Especialmente no que se refere à possibilidade de exigência do documento na hipótese de tratamento fundamentado na base legal do legítimo interesse, há de se consignar que a própria redação do art. 10, § 3º da LGPD indica que a ANPD *poderá* exigir o documento[109], o que significa que não seria, necessariamente, uma condição obrigatória para o tratamento de dados fundamentado na base legal do legítimo interesse.

Ainda, se considerada a própria definição de Relatório de Impacto constante no artigo 5º, XVII da LGPD[110], que indica a opção da Lei pela metodologia baseada em risco para a elaboração do documento, não seria necessária a elaboração de Relatório de Impacto em qualquer operação que esteja fundamentada na base legal do legítimo

---

[108] TIMM, Luciano; CAOVILLA, Renato; STURARI, Mateus. O Relatório de Impacto na LGPD: Sentido e Limites Dentro da Regulação Econômica. *In*: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coords.). **Proteção de Dados:** Temas Controvertidos. Indaiatuba: Editora Foco, 2021, pp. 362-384.

[109] Art. 10, § 3º (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

[110] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022.

interesse ou que envolva o tratamento de dados sensíveis, mas somente naquelas que imponham alto risco aos direitos e liberdades dos titulares[111].

Assim, mesmo que o tratamento de dados sensíveis, em razão da categoria delicada dos dados tratados, possa indicar possível risco elevado aos titulares, o cerne da identificação de hipóteses que demandariam a elaboração do documento está na identificação de atividades de tratamento de alto risco, motivo pelo qual, no próximo capítulo, são analisados alguns subsídios interpretativos para a identificação de atividades de tratamento de alto risco, bem como a atuação da ANPD na regulamentação específica do tema.

3.2 SUBSÍDIOS INTERPRETATIVOS E ATUAÇÃO DA ANPD

Os artigos 38 e 55-J, inciso XIII, da LGPD deixam claro que caberá à ANPD a exigência de Relatórios de Impacto dos controladores, bem como caberá a ela a regulamentação do tema, incluindo, portanto, a definição de parâmetros para identificação de atividades de alto risco que demandariam a elaboração do documento pelos controladores[112].

No entanto, até o momento da escrita da presente monografia, a ANPD ainda não expediu nenhum guia orientativo ou regulamento específico sobre Relatórios de Impacto, de modo que sua atuação se limitou à realização de três reuniões técnicas para discutir o documento, nos dias 21, 23 e 25 de junho.

Em tais reuniões sediadas pela Autoridade, alguns pontos sobre o Relatório de Impacto foram discutidos pelos debatedores. Durante o primeiro dia, foi abordado que, a partir de uma análise interpretativa da Lei, conclui-se que a LGPD propõe uma abordagem baseada em riscos para identificação dos casos nos quais seria necessário elaborar Relatório de Impacto, vez que tais documentos são ferramentas de avaliação e gerenciamento de riscos. No entanto, como a Lei não explora as

---

[111] RUIZ, Juliana Pacetta; FRANCO, Sofia Lima. Gestão de Risco em Projetos de Adequação: Benefícios e Desafios de uma Abordagem Baseada em Risco na LGPD. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, p. 513-544, p. 533.

[112] Art. 38, e art. 55-J, XIII (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

definições de risco, o debate sobre quando um processo de tratamento seria considerado de “alto risco” é central no que se refere à análise da matéria[113].

Antes de adentrar na conceituação de risco e formas de identificar atividades de tratamento que estariam sujeitas à elaboração de Relatório de Impacto, cabe refletir brevemente sobre a obrigatoriedade do documento no contexto brasileiro.

Os artigos que expressamente mencionam o Relatório de Impacto na LGPD não indicam que o documento seria obrigatório, apenas referem que a ANPD, em alguns casos, pode vir a solicitar esses documentos dos controladores. Assim, a partir de uma análise mais restritiva, pode-se concluir que o Relatório de Impacto seria apenas uma recomendação para o controlador mitigar os riscos da atividade e uma das formas de buscar conformidade com a LGPD[114].

Por outro lado, se consideradas as expressões “pode *determinar*” e “pode *exigir*” constantes nos artigos 38 e 10º, §3º, da LGPD[115], a elaboração de Relatórios de Impacto não seria mera liberalidade dos controladores, mas sim exigência ou determinação da Autoridade Nacional, que, por ser o órgão competente inclusive para impor sanções a agentes que descumpram a LGPD, *deve* ser observada pelos agentes de tratamento para que estejam em conformidade com a Lei.

Certo é que, independentemente de ser compreendido como documento obrigatório ou não, os controladores devem elaborar Relatório de Impacto antes de eventual exigência específica pela ANPD. Assim, mostra-se essencial a construção de alguma metodologia para a identificação das situações em que a elaboração do documento pelo controlador seria necessária ou exigível pela ANPD.

Partindo da própria definição e finalidade do Relatório de Impacto trazidas pela Lei[116], bem como da conclusão apontada nas reuniões técnicas promovidas pela

---

[113] GARROTE, Marina Gonçalves *et. al.* ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais. **Jota**, [*S.l.*], 13 jul. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 22 abr. 2022.

[114] GOMES, Maria Cecília Oliveira. Para além de uma “obrigação legal”: o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In:* LIMA, Ana Paula; HISSA, Carmina; SALDANHA, Paloma Mendes (Orgs.). **Direito Digital:** Debates Contemporâneos. São Paulo: Revista dos Tribunais, 2019, pp. 141-153.

[115] Art. 38, e art. 10º, §3º (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

[116] Relatório de Impacto à Proteção de Dados trata-se da documentação do controlador destinada a descrever os processos de tratamento de dados que podem causar riscos às liberdades civis e direitos fundamentais dos titulares e a indicar medidas, salvaguardas e mecanismos de mitigação de risco. Art. 5º, XVII (BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de

ANPD, pode-se concluir que a LGPD propôs uma abordagem baseada em risco para a elaboração do Relatório de Impacto[117].

Assim, para que seja possível refletir sobre as hipóteses que demandariam a elaboração do Relatório de Impacto, é necessária a conceituação de risco na LGPD.

A partir de uma definição dúplice de risco, tem-se que o risco é determinado pela cominação de um determinado evento e suas possíveis consequências. Trata-se, portanto, de uma previsão, a partir da análise de um evento, de eventos futuros tanto negativos como positivos. A avaliação de risco, por sua vez, pode ser dividida em três partes: o reconhecimento dos riscos que podem prejudicar uma organização a alcançar seus objetivos, a compreensão da natureza desse risco e a determinação de ações para mitigá-lo[118].

Apesar da relevância da conceituação de risco, especialmente para fins de identificação das hipóteses de tratamento de dados que demandariam a elaboração de Relatório de Impacto, a LGPD não prevê uma definição para risco e fornece poucos parâmetros para sua avaliação. E mesmo as atividades que a LGPD sinaliza que poderão oferecer maior risco, como o caso de tratamento de dados sensíveis, não necessariamente apresentam elevado risco sempre. Isso porque, o risco varia de acordo com o contexto de tratamento de dados, razão pela qual fatores como natureza dos dados, quantidade de dados objeto de tratamento, categoria dos titulares e forma de tratamento devem ser considerados conjuntamente para avaliação de risco das operações[119].

Ainda, há de se pontuar que o risco não pode ser quantificado, vez que é constituído por características qualitativas e valorativas. Ou seja, é possível atribuir ao

---

Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022).

117 GARROTE, Marina Gonçalves *et. al.* ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais. **Jota**, [*S.l.*], 13 jul. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 22 abr. 2022.

118 MENKE, Fabiano; GARCIA, Rafael Scaroni. Análise de Risco sobre Proteção de Dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 548-550.

119 RUIZ, Juliana Pacetta; FRANCO, Sofia Lima. Gestão de Risco em Projetos de Adequação: Benefícios e Desafios de uma Abordagem Baseada em Risco na LGPD. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, p. 513-544, p. 516.

risco indicadores como “alto, médio e baixo”, mas não indicadores quantitativos, como porcentagens de risco identificadas nas operações[120].

E, como a LGPD não prevê critérios objetivos que identifiquem operações de tratamento de dados de alto risco, tal avaliação dos riscos das atividades cabe aos agentes de tratamento que por elas são responsáveis.

Para avaliar os riscos inerentes às atividades de tratamento que realizam, o primeiro passo a ser seguido pelos agentes de tratamento é o mapeamento das operações que envolvem o tratamento de dados pessoais. Nesse ponto, é importante que o mapeamento contemple informações importantes para a posterior classificação das atividades como de alto risco, tais como: tipo de atividade realizada; quantidade de dados tratados; categoria dos titulares dos dados; natureza dos dados; número de titulares afetados; finalidade do tratamento; mecanismos técnicos utilizados para o tratamento; bem como o impacto que o tratamento pode causar nos direitos e liberdades dos titulares[121].

Após o mapeamento das operações de tratamento de dados, cabe aos agentes de tratamento a identificação, entre as atividades mapeadas, de quais atividades seriam consideradas como de alto risco aos titulares dos dados tratados.

Nesse ponto, como a ANPD ainda não expediu regulamentação ou orientação específica sobre o tema, para fins de avaliação das operações que seriam consideradas como de alto risco, os agentes de tratamento podem se utilizar da definição de tratamento de alto risco emitida pela ANPD no regulamento de aplicação da LGPD para Agentes de Pequeno Porte, aprovado em resolução CD/ANPD nº 2, de 27 de janeiro de 2022[122].

Apesar de especificamente tratar sobre a aplicação da LGPD aos agentes de pequeno porte, o regulamento prevê, em seu artigo 4º, a definição de tratamento de alto risco, que pode servir como importante ferramenta para a identificação, pelos

---

120 GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In:* PALHARES, Felipe (Coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020, pp. 245-271.

121 RUIZ, Juliana Pacetta; FRANCO, Sofia Lima. Gestão de Risco em Projetos de Adequação: Benefícios e Desafios de uma Abordagem Baseada em Risco na LGPD. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, p. 513-544, p. 529-530.

122 BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022.

agentes de tratamento, das operações que demandariam a elaboração de Relatório de Impacto em razão de seu alto risco.

De acordo com o artigo 4º do regulamento, será considerado de alto risco o tratamento de dados que atender simultaneamente a, pelo menos, um critério geral e um específico indicados no próprio artigo. Como critérios gerais, o regulamento aponta os seguintes: i) tratamento em larga escala e ii) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares. A título de critérios específicos, foram apontados: i) uso de tecnologias emergentes ou inovadoras; ii) vigilância ou controle de zonas acessíveis ao público; iii) decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais, incluindo a definição de perfis dos titulares; e iv) utilização de dados sensíveis ou dados de crianças, adolescentes e idosos[123].

Quanto ao tratamento em larga escala, o próprio regulamento, no parágrafo 1º do artigo 4º, prevê que serão considerados de larga escala tratamentos de dados que abranger um número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, a duração, a frequência e extensão do tratamento[124].

Já o tratamento de dados que pode afetar os direitos fundamentais e interesses dos titulares é caracterizado pelas situações em que a atividade de tratamento possa impedir o exercício de direitos ou utilização de um serviço pelos titulares, bem como ocasionar danos materiais ou morais aos titulares, como discriminação, violação à integridade física, direito à imagem e à reputação, fraudes financeiras ou roubo de identidade, conforme definição do parágrafo 2º do artigo 4º do regulamento[125].

Assim, a partir da análise das definições emitidas pela ANPD no regulamento, percebe-se que, mesmo que tenham sido elaboradas no contexto de regulamentação

---

[123] Art. 4º (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).

[124] Art. 4º, § 1º (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).

[125] Art. 4º, § 2º (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).

da aplicação da LGPD a agentes de pequeno porte, os critérios guardam substanciais semelhanças com aqueles apresentados no guia orientativo do *Article 29 Working Party* da União Europeia sobre Relatórios de Impacto, documento que foi objeto de análise no capítulo anterior.

Veja-se que o primeiro dos dois critérios gerais previstos pela ANPD no Regulamento é o tratamento de dados em larga escala[126], que, por sua vez, também foi previsto pelo *Article 29 Working Party* no guia orientativo sobre DPIA como o quinto critério para identificação de operações de alto risco[127].

Já o segundo critério geral previsto no Regulamento da ANPD, tratamento de dados capaz de afetar significativamente direitos e interesses dos titulares[128], definido pelo próprio Regulamento como aquelas situações nas quais a atividade de tratamento pode impedir o exercício de direitos ou utilização de serviços pelos titulares, bem como ocasionar danos materiais ou morais aos titulares[129], é semelhante ao nono critério presente no guia orientativo sobre DPIA elaborado pelo *Article 29 Working Party*[130].

Nesse mesmo sentido, percebe-se que todos os demais critérios específicos previstos pela ANPD no Regulamento também estão presentes no trabalho do *Article 29 Working Party.*

O primeiro critério específico previsto pelo Regulamento, uso de tecnologias emergentes ou inovadoras, equivale ao oitavo critério previsto pelo guia orientativo do

---

126 Art. 4º, I, a (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).

127 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

128 Art. 4º, I, b (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).

129 Art. 4º, § 2º (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).

130 UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

Article 29 Working Party; já o segundo critério, vigilância ou controle de zonas acessíveis ao público, guarda substanciais semelhanças com o terceiro critério previsto pelo guia orientativo do *Article 29 Working Party*. O terceiro critério específico do Regulamento da ANPD, decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir perfis, por sua vez, equivale ao segundo critério previsto pelo *Article 29 Working Party* em seu guia orientativo. Por fim, o critério de utilização de dados sensíveis ou de dados pessoais de crianças, adolescentes e idosos do Regulamento da ANPD é uma combinação do quarto e sétimo critérios previstos pelo órgão consultivo da União Europeia[131].

Tais equivalências encontram-se resumidas e ilustradas no quadro 2, a seguir:

Quadro 2: Equivalência entre os critérios previstos no Regulamento da ANPD e aqueles previstos no guia orientativo sobre DPIA do *Article 29 Working Party*

Critérios previstos pelo Regulamento de aplicação da LGPD para Agentes de Pequeno Porte, expedido pela ANPD	**Respectivos critérios previstos no Guia Orientativo do *Article 29 Working Party* sobre DPIA**
Art. 4º, I, "a" do Regulamento: Tratamento de dados pessoais em larga escala	Critério 5 do guia orientativo sobre DPIA: Dados tratados em larga escala
Art. 4º, I, "b" do Regulamento: Tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares Art. 4º, § 2º, do Regulamento: O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de serviços pelos titulares	Critério 9 do guia orientativo sobre DPIA: Tratamento de dados que, em si mesmo, impede ou dificulta o exercício de um direito pelo titular ou o uso de um serviço ou contratação
Art. 4º, II, "a" do Regulamento: Uso de tecnologias emergentes ou inovadoras	Critério 8 do guia orientativo sobre DPIA: Uso ou aplicação inovadora de novas tecnologias ou soluções organizacionais
Art. 4º, II, "b" do Regulamento: vigilância ou controle de zonas acessíveis ao público	Critério 3 do guia orientativo sobre DPIA: Monitoramento sistemático, incluindo

[131] Art. 4º (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).
UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

	monitoramento de uma área publicamente acessível
Art. 4º, II, “c” do Regulamento: Decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive para fins de definição de perfis	Critério 2 do guia orientativo sobre DPIA: Decisões automatizadas com efeitos jurídicos ou similares
Art. 4º, II, “d” do Regulamento: utilização de dados sensíveis ou de dados pessoais de crianças, adolescentes e idosos	Critério 4 do guia orientativo sobre DPIA: Tratamento de dados sensíveis ou de natureza altamente pessoal Critério 7 do guia orientativo sobre DPIA: Tratamento de dados de titulares vulneráveis

Fonte: Elaborado pela autora (2022)[132].

Ainda, além das semelhanças entre os critérios para identificação de atividades de alto risco previstos no Regulamento expedido pela ANPD e aqueles critérios presentes no guia orientativo do *Article 29 Working Party* sobre DPIA, percebe-se clara semelhança entre a definição de tratamento em larga escala prevista no art. 4º, § 1ª do Regulamento da ANPD[133] e a definição de tratamento em larga escala presente no *Guidelines on Data Protection Officers,* também elaborado pelo *Article 29 Working Party* no âmbito do desenvolvimento do tema na União Europeia[134].

Isso porque, em ambos os casos, o número significativo de titulares, volume de dados tratados, duração e extensão geográfica da atividade de tratamento são apontados como fatores a serem considerados para a classificação de uma atividade de tratamento como de larga escala.

---

[132] Quadro elaborado pela autora a partir da análise do Regulamento de Aplicação da LGPD para Agentes de Pequeno Porte expedido pela ANPD (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022) e do documento Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022).

[133] Art. 4º, § 1º (BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022).

[134] UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

Assim, considerando a substancial semelhança entre as previsões sobre tratamento de alto risco constantes no Regulamento de aplicação da LGPD para Agentes de Pequeno porte expedido pela ANPD e as orientações expedidas pelo *Article 29 Working Party* na União Europeia para fins de identificação de atividades que demandam a elaboração de DPIA, bem como a opção pela Lei brasileira pela metodologia de risco para a exigência do Relatório de Impacto, pode-se concluir que as previsões sobre tratamento de alto risco do Regulamento da ANPD podem, e talvez até devam, ser utilizadas pelos agentes de tratamento no contexto brasileiro para identificação das hipóteses que demandariam a elaboração de Relatório de Impacto.

Também é possível concluir, a partir da análise comparativa realizada, que a ANPD tem demonstrado adotar metodologias bastante semelhantes com aquelas utilizadas no âmbito da União Europeia para a definição de tratamento de alto risco, o que é um indicativo de que os trabalhos elaborados pelo órgão da União Europeia podem orientar a futura atuação da ANPD na regulamentação específica sobre os Relatórios de Impacto.

4 CONCLUSÃO

Em razão da ausência de regulamentação específica sobre os Relatórios de Impacto pela Autoridade Nacional de Proteção de Dados brasileira, especialmente no que tange à definição de critérios para orientar a identificação, pelos controladores, das hipóteses de tratamento de dados que demandariam a elaboração de tais documentos, o presente trabalho se propôs a identificar possíveis parâmetros que podem ser observados pela ANPD quando da regulamentação do tema.

Para isso, e considerando a semelhança entre a LGPD e o GDPR, um dos subsídios para o desenvolvimento do presente estudo foi a análise da experiência europeia. Além disso, e a fim de avaliar se as orientações e metodologias desenvolvidas no âmbito da União Europeia podem ser aproveitadas no contexto brasileiro, foi realizada uma análise sistemática dos contornos brasileiros existentes sobre a temática.

A partir da análise das definições presentes no GDPR, constatou-se que a legislação europeia elegeu a metodologia baseada em risco para a identificação de operações de tratamento de dados que demandariam a elaboração de DPIA. Assim, seria necessário elaborar DPIA no caso de operações que apresentem alto risco aos titulares de dados.

Verificou-se que no próprio texto do GDPR há a previsão de algumas hipóteses de exigência de elaboração do DPIA, bem como importantes esclarecimentos interpretativos em alguns de seus considerandos. Também foi objeto de análise o trabalho do *Article 29 Working Party*, um dos principais reforços acerca do tema no âmbito da União Europeia.

O documento *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk for the purposes of Regulation 2016/679* contém importantes diretrizes interpretativas e esclarecimentos acerca do tema e estabelece uma metodologia baseada em nove critérios, quais sejam: i) operações de avaliação ou classificação; ii) decisões automatizadas que produzam efeitos jurídicos à pessoa natural ou a afetem significativamente de modo similar; iii) monitoramento sistemático; iv) dados sensíveis ou dados de natureza altamente pessoal, o que inclui dados relacionados a condenações penais; v) dados tratados em larga escala; vi) combinação de dados originados de diferentes operações de tratamento; vii) dados de titulares vulneráveis; viii) uso ou aplicação de soluções

tecnológicas ou organizacionais inovadoras; e ix) tratamento de dados que, em si, impede os titulares de exercer um direito ou usar um serviço ou contrato[135].

A combinação de, pelo menos, dois critérios indicaria alto risco da operação de tratamento de dados, o que ensejaria a necessidade de elaboração de DPIA pelo controlador.

Apesar de não ser uma regra absoluta e objetiva, vez que o próprio guia orientativo ressalva que, eventualmente, operações que contemplem apenas um dos critérios também podem ser consideradas de alto risco pelo controlador, ao se analisar os nove critérios comparativamente às hipóteses de exigência do DPIA previstas no texto legal do GDPR, verificou-se que é realmente lógico que a combinação de, pelo menos, dois critérios em uma operação de tratamento indique potencial elevado de risco aos direitos e liberdades dos titulares. Isso porque, alguns dos critérios combinados entre si são derivações mais detalhadas dos próprios exemplos previstos no parágrafo terceiro do artigo 35 do GDPR, o que demonstra a efetividade e compatibilidade do método proposto pelo *Article 29 Working Party* com as disposições do GDPR.

A fim de esclarecer importantes conceitos-chave para a identificação dos critérios propostos pelo *Article 29 Working Party*, analisou-se, também, as definições de tratamento sistemático de dados e tratamento de dados em larga escala, presentes no documento denominado *Guidelines on Data Protecion Officers,* também elaborado pelo *Article 29 Working Party.*

Ainda, a fim de complementar o estudo da experiência europeia no desenvolvimento do tema e verificar a aplicabilidade prática da metodologia baseada em critérios proposta pelo *Article 29 Working Party*, foi realizada uma análise do histórico de sanções administrativas impostas pelas Autoridades Nacionais de proteção de dados da União Europeia em razão da ausência de elaboração de DPIA pelos controladores.

Como conclusão do estudo de casos, identificou-se que as operações de tratamento de dados em relação às quais as Autoridades identificaram ser necessária a elaboração de DPIA são condizentes com os critérios definidos pelo *Article 29*

---

[135] UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

Working Party, o que demonstra que a metodologia proposta pelo órgão consultivo tem sido utilizada na prática da fiscalização das Autoridades Nacionais.

No que se refere ao desenvolvimento do tema no contexto brasileiro de proteção de dados, foram analisados dispositivos legais, interpretações doutrinárias e atuação da ANPD no desenvolvimento do tema. A partir disso, concluiu-se que, nos moldes do GDPR, a LGPD optou por uma metodologia baseada em risco para identificação das hipóteses de exigência de elaboração do Relatório de Impacto pelos controladores de dados.

Diante disso, e considerando que a própria definição de tratamento de dados de alto risco prevista pela ANPD em regulamento expedido sobre aplicação da LGPD para agentes de pequeno porte guarda substanciais semelhanças com os critérios previstos no guia orientativo do *Article 29 Working Party* sobre DPIA, é possível concluir que a Autoridade Nacional de Proteção de Dados, ao regulamentar a matéria no contexto brasileiro, pode utilizar a metodologia proposta no *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk for the purposes of Regulation 2016/679* como subsídio para construir suas orientações.

Claro que, assim como no próprio contexto da União Europeia, eventual lista de critérios ou metodologia estabelecida pela ANPD não poderá se tratar de um rol taxativo de hipóteses de operações de tratamento de dados que demandam a elaboração de Relatório de Impacto. Isso porque, apesar de ser um cenário que forneceria maior grau de segurança jurídica aos agentes de tratamento de dados, em razão da própria dinamicidade das atividades que envolvem o tratamento de dados pessoais, bem como o rápido aperfeiçoamento das tecnologias utilizadas para esses tipos de operações, é impossível pré-estabelecer um rol taxativo de atividades que apresentariam elevado risco aos titulares.

Ora, é possível que eventuais operações de tratamento de dados que possam gerar alto risco sequer existam no momento do estabelecimento de uma lista pela Autoridade Nacional, vez que todos os dias novas operações de tratamento de dados são realizadas com base em novas tecnologias que estão sendo desenvolvidas[136].

---

[136] GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In:* PALHARES, Felipe (Coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020, pp. 245-271.

Assim, longe de propor soluções simplistas a um tema complexo e subjetivo, o presente estudo conclui que a experiência europeia no estabelecimento de metodologia para a identificação de hipóteses de operações de tratamento de dados de alto risco aos titulares de dados pode auxiliar a Autoridade Nacional na construção de um documento que, apesar de não apresentar um rol taxativo de atividades que demandariam a elaboração de relatório de impacto, pode trazer importante segurança jurídica aos agentes de tratamento de dados no contexto de desenvolvimento de uma cultura de proteção de dados brasileira.

REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo; GOMES, Maria Cecilia Oliveira; MONTEIRO, Renato Leite. GDPR matchup: Brazil's General Data Protection Law. **IAPP,** Portsmouth, 04 out. 2019. Disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Acesso em: 22 abr. 2022.

BIONI, Bruno Ricardo; MENDES, Laura Schertel. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, v. 124, pp. 157-180, jul./ago. 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 791-814.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr. 2022.

BRASIL. Presidência da República. **Resolução CD/ANPD n. 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, DF: Presidência da República, [2022]. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 22 abr. 2022.

DONEDA, Danilo; MENDES, Laura. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, nov./dez. 2018.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 23-52.

GARROTE, Marina Gonçalves *et. al.* ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais. **Jota**, [*s.//.*], 13 jul. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 22 abr. 2022.

GDPR Enforcement Tracker. [**Homepage**]. [*s./l*], 2022. Disponível em: https://www.enforcementtracker.com/. Acesso em: 22 abr. 2022.

GELLERT, Raphael. EDPB Opinion on the Draft Lists of Competent Supervisory Authorities regarding the Processing Operations Subject to DPIAs. **European Data Protection Law Review**, n. 4, pp. 500-504, Berlim, 2018.

GELLERT, Raphael. The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment. **European Data Protection Law Review**, n. 2, pp. 212-217, Berlim, 2017.

GOMES, Maria Cecília Oliveira. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In:* LIMA, Ana Paula; HISSA, Carmina; SALDANHA, Paloma Mendes (Orgs.). **Direito Digital:** Debates Contemporâneos. São Paulo: Revista dos Tribunais, 2019, pp. 141-153.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados: Uma breve análise da sua definição e papel na LGPD. **Revista do Advogado**, São Paulo, ano 39, n. 144, pp. 174-183, nov. 2019.

GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In:* PALHARES, Felipe (Coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020, pp. 245-271.

GOMES, Maria Cecília Oliveira. LGPD: Desafios da regulamentação do relatório de impacto. **Jota**, [*S./l.*], 11 fev. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. Acesso em: 22 abr. 2022.

HAYDUK, Gabriel. Requisitos do Relatório de Impacto à Proteção de Dados Pessoais. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, p.569 - 585.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019.

MENKE, Fabiano; GARCIA, Rafael Scaroni. Análise de Risco sobre Proteção de Dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 548-550.

POLIDO, Fabricio *et. al.* **GDPR e suas repercussões no direito brasileiro**: primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade – IRIS: Belo Horizonte, 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%c3%b5es-no-direito-brasileiro-

Primeiras-impress%c3%b5es-de-an%c3%a1lise-comparativa-PT.pdf. Acesso em: 22 abr. 2022.

RUIZ, Juliana Pacetta; FRANCO, Sofia Lima. Gestão de Risco em Projetos de Adequação: Benefícios e Desafios de uma Abordagem Baseada em Risco na LGPD. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Coords.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021, p. 513-544.

Sobre a definição, ver website do European Data Protection Board. UNIÃO EUROPEIA. Comissão Europeia. Article 29 Working Party. **European Data Protection Board**. Bruxelas, [*s./d*.]. Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en. Acesso em: 22 abr. 2022.

TIMM, Luciano; CAOVILLA, Renato; STURARI, Mateus. O Relatório de Impacto na LGPD: Sentido e Limites Dentro da Regulação Econômica. *In*: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Coords.). **Proteção de Dados:** Temas Controvertidos. Indaiatuba: Editora Foco, 2021, pp. 362-384.

UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016. **Official Journal of the European Union**, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 22 abr. 2022.

UNIÃO EUROPEIA. **Article 29 working party, composition & structure**. Bruxelas, 06 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/605262/en. Acesso em: 22 abr. 2022.

UNIÃO EUROPEIA. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. WP248.** Bruxelas, 13 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 22 abr. 2022.

UNIÃO EUROPEIA. **Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)**. Bruxelas, 30 out. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612048/en. Acesso em: 22 abr. 2022.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados (RGPD, GDPR)**. Considerandos n. 75, 89 e 91. Bruxelas, 2018. Disponível em: https://gdpr-text.com/pt/read/article-35/#recital. Acesso em: 22 abr. 2022.

UNIÃO EUROPEIA. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)**. Bruxelas, 22 ago. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 22 abr. 2022.

UNIÃO EUROPEIA. Who we are. **European Data Protection Board.** Bruxelas, [*s./d*.]. Disponível em: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en. Acesso em: 22 abr. 2022.

WILLS, Leonard. A Very Brief Introduction to the GDPR Recitals. **Minority Trial Lawyer**, v. 17, n. 1, p. 15-16, maio 2019. Disponível em: https://heinonline.org/HOL/Page?public=true&handle=hein.aba/mitril0017&div=8&start_page=15&collection=trials&set_as_cursor=0&men_tab=srchresults. Acesso em: 22 abr. 2022.