

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

LARA SOARES MIRANDA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS: UM ESTUDO COMPARADO
ENTRE O DIREITO BRASILEIRO E O EUROPEU

UBERLÂNDIA/MG

2021

LARA SOARES MIRANDA

RELATÓRIO DE IMPACTO À PROTEÇÃO DA DADOS: UM ESTUDO COMPARADO
ENTRE O DIREITO BRASILEIRO E O EUROPEU

Trabalho de conclusão de curso apresentado à
Faculdade de Direito da Universidade Federal
de Uberlândia como requisito parcial para
obtenção do título de Bacharel em Direito

Orientador: Prof. Dr. Rodrigo Vitorino Souza
Alves

UBERLÂNDIA/MG

2021

LARA SOARES MIRANDA

RELATÓRIO DE IMPACTO À PROTEÇÃO DA DADOS: UM ESTUDO COMPARADO
ENTRE O DIREITO BRASILEIRO E O EUROPEU

Trabalho de Conclusão de Curso apresentado à
Faculdade de Direito da Universidade Federal
de Uberlândia como requisito parcial para
obtenção do título de bacharel em Direito

Uberlândia, 14 de outubro de 2021.

Banca Examinadora:

Rodrigo Vitorino Souza Alves – Orientador, Professor Doutor na UFU

João Alexandre Guimarães – Professor da Faculdade Pitágoras, Doutorando em Direito pela
Universidade de Coimbra

Juliana Gomes Pinto Borges – Professora da ESAMC

RESUMO

O relatório de impacto à proteção de dados pessoais é um documento complexo, que deve ser elaborado a partir da utilização de uma metodologia específica, quando o tratamento de dados pessoais representa riscos aos direitos fundamentais e às liberdades dos indivíduos. Ele é previsto em diversos países e as autoridades nacionais regulamentam o tema e direcionam a metodologia de elaboração do documento. Em um primeiro momento é feita uma análise minuciosa da previsão legal do relatório de impacto na lei brasileira e na europeia, bem como das instruções práticas para elaboração do documento e das decisões sobre tema. O ponto central da presente pesquisa é atingido em um segundo momento, com a realização de estudo comparado da previsão legal do relatório de impacto na Lei Geral de Proteção de Dados e no Regulamento Geral de Proteção de Dados, observando a metodologia funcionalista moderada, que busca identificar as semelhanças e diferenças entre os ordenamentos jurídicos analisados.

Palavras-chave: Relatório de impacto. Direitos fundamentais. Estudo comparado

ABSTRACT

The Data protection impact assessment is a very complex document, that must be created with employment of a specific methodology when the personal data treatment represents risks to the individuals fundamental rights and their freedom. The document exists in many countries and the national authorities regulates the subject and guide the document elaboration methodology. At the first moment a careful analysis about the impact assessment legal prediction in Brazilian and European laws is done as well the practices instructions for the document elaboration and decisions about the subject. The main point of the present research is reached in a second moment with the impact assessment legal prediction in Data Protection General law and General Data Protection Regulation comparative study observing the moderate functionalist methodology that identify the similarities and the differences between the analyzed laws.

Keywords: Impact assessment. Fundamental rights. Comparative study

LISTA DE TABELAS

Tabela 1 -	Cronograma da ANPD sobre as reuniões técnicas.....	16
Tabela 2 -	Tópicos do despacho ministerial do MPDFT.....	19
Tabela 3 -	Modelo do EDPS para avaliação de impacto.....	26
Tabela 4 -	Tabela comparativa sobre o relatório de impacto.....	30

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
DPIA	<i>Data Protection Impact Assessment</i>
EDPS	<i>European Data protection supervisor</i>
GDPR	<i>General Data Protection Regulation</i>
LGPD	Lei Geral de Proteção de Dados
MPDFT	Ministério Público do Distrito Federal e Territórios
RIPD	Relatório de impacto à proteção de dados

Sumário

1. INTRODUÇÃO.....	8
2. O RELATÓRIO DE IMPACTO NA LGPD	10
2.1. A PREVISÃO LEGAL DO RELATÓRIO DE IMPACTO NA LGPD.....	10
2.2. A ELABORAÇÃO DO RELATÓRIO DE IMPACTO.....	15
2.3. DECISÕES BRASILEIRAS SOBRE O TEMA	18
3. O RELATÓRIO DE IMPACTO NO GDPR.....	21
3.1. A PREVISÃO LEGAL DA AVALIAÇÃO DE IMPACTO NO GDPR	21
3.2. A ELABORAÇÃO DA AVALIAÇÃO DE IMPACTO	25
3.3. DECISÕES EUROPEIAS SOBRE O TEMA	27
4. COMPARATIVO ENTRE A PREVISÃO EUROPEIA E A BRASILEIRA.....	28
5. CONSIDERAÇÕES FINAIS	30

1. INTRODUÇÃO

O presente estudo tem como tema o relatório de impacto à proteção de dados¹ (RIPD) e será realizado a partir da comparação entre o Direito Brasileiro e o Direito Europeu, com enfoque nas legislações que tratam da proteção de dados pessoais, sendo a Lei Geral de Proteção de Dados (LGPD) brasileira e o *General Data Protection Regulation*² (GDPR) europeu, que entrou em vigor em 2018³ e estimulou os outros países a criarem suas Leis de Proteção de Dados.

Para melhor entendimento do relatório de impacto é necessária a compreensão da trajetória histórica que culminou na criação da LGPD no Brasil. Sabe-se que as discussões acerca da proteção de dados no Brasil iniciaram-se em 2010⁴, com o seminário organizado pelo Comitê Gestor da Internet. Desse momento em diante, muitos acontecimentos marcantes impulsionaram a criação de uma lei específica, que regulamentasse o tratamento de dados pessoais pelo setor público e privado, como o escândalo de espionagem do Edward Snowden em 2014, a entrada em vigor do Marco Civil da Internet e o caso de manipulação de dados pela Cambridge Analytica em 2018, que revelou a grande influência nas eleições presidenciais dos Estados Unidos e no *Brexit* da Inglaterra.

Foram realizadas três consultas públicas envolvendo o setor privado, a sociedade civil e a academia, razão pela qual se pode dizer que a LGPD é uma lei democrática, que foi criada com a participação de todos os setores da sociedade, após diversas audiências públicas, em que houve debate acerca das diferentes demandas dos três setores.

Apesar de o Poder Legislativo brasileiro ter buscado inspiração no GDPR, existem algumas diferenças em suas técnicas normativas, sendo que a primeira delas é o fato de a legislação brasileira ser menos prescritiva⁵ e não possuir os “Considerandos”, presentes no GDPR, que têm a função de orientar a interpretação do texto legal, trazendo explicações muito

¹ Definição no Art. 5º, XVII da LGPD: “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.”

² Que em português significa Regulamento Geral sobre a Proteção de Dados.

³ “É certo que o Regulamento é relativamente novo, pois sua efetiva aplicação iniciou-se em maio de 2018. (BORELLI et al., 2020, p. 18).

⁴ DATAPRIVACYBR. Memória da LGPD. 2020. Disponível em: <https://www.observatorioprivacidade.com.br/memorias/>. Acesso em: 25 maio 2021.

⁵ MONTEIRO, Renato Leite. GDPR matchup: Brazil's General Data Protection Law. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 25 maio 2021.

relevantes, principalmente para os momentos em que somente a análise da legislação não é suficiente para a resolução de problemas em um caso concreto.

Em relação à previsão do relatório de impacto, há diferenças entre a legislação brasileira e a europeia, como a não previsão expressa na LGPD acerca da necessidade de acompanhamento do relatório de impacto à proteção de dados pelo encarregado⁶ e da consulta prévia à Autoridade Nacional de Proteção de Dados (ANPD), antes do início de uma operação de dados que demonstre elevado risco.

Com a vigência da lei, a Autoridade Nacional de Proteção de Dados⁷ agendou reuniões técnicas para coletar informações dos especialistas sobre o relatório de impacto à proteção de dados, a fim de que o órgão pudesse responder algumas perguntas relevantes, como quais serão as metodologias adequadas, os elementos necessários, como será feita a avaliação, qual será a definição de alto risco, a previsão de um prazo de entrega razoável do relatório, entre outras questões.

Para Monteiro⁸, enquanto não forem estipuladas definições pela Autoridade Nacional de Proteção de Dados, uma possível alternativa é que o direito brasileiro tenha como base o *Data Protection Impact Assessment* (DPIA) da União Europeia e utilize como modelo os documentos disponibilizados pelos órgãos de proteção de dados para elaboração de seu relatório de Impacto.

Diante disso, esse estudo realizará uma análise sobre o relatório de Impacto à proteção de dados nos momentos em que é citado na LGPD⁹, quanto à sua definição, seus atores, sua aplicabilidade e suas exigências e a possibilidade de sua adoção em outros momentos não descritos na legislação, também o estudo da importância da elaboração, pelos controladores¹⁰ de dados, do relatório de Impacto. Para Lima et al.¹¹, o documento tem a função de minimizar os riscos aos dados pessoais e até mesmo eliminar os processos que causam ameaças, de forma que haja uma justificativa para os riscos que permanecerem nas Instituições e a estimulação de

⁶ (LIMA et al., 2019)

⁷ “A Autoridade Nacional de Proteção de Dados (ANPD) abriu hoje, dia 25/05, as inscrições para participação de especialistas em suas reuniões técnicas sobre relatório de impacto de proteção de dados pessoais.” ANPD (2021)

⁸ MONTEIRO, Renato Leite. GDPR matchup: Brazil's General Data Protection Law. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 25 maio 2021.

⁹ O Relatório de Impacto à Proteção de Dados é citado seis vezes na LGPD.

¹⁰ A responsabilidade dos Controladores está descrita no Art. 38 da LGPD: “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.”

¹¹ LIMA, Adriano Carlos de et al. LGPD - Lei Geral de Proteção de Dados: manual de implementação. São Paulo: Thomson Reuters, 2019. 368 p. Coordenação de Viviane Nóbrega Maldonado.

uma cultura de proteção de dados¹², não só no meio corporativo, mas na sociedade, reforçando a importância da criação do relatório de impacto à proteção de dados, principalmente porque ele refere-se a tratamentos de dados que podem acarretar riscos aos direitos fundamentais dos indivíduos.

Sendo assim, o presente estudo comparado do relatório de impacto à proteção de dados na legislação brasileira e na europeia será realizado a partir da metodologia funcionalista moderada, que compreende tanto as semelhanças quanto as diferenças entre os ordenamentos jurídicos e pressupõe uma decisão sobre o enfoque da comparação somente após a pesquisa concreta dos ordenamentos.

2. O RELATÓRIO DE IMPACTO NA LGPD

2.1. A PREVISÃO LEGAL DO RELATÓRIO DE IMPACTO NA LGPD

Existem seis momentos em que o relatório de impacto é mencionado na LGPD. A primeira menção¹³ ocorre no Art. 4º, § 3º, com a previsão de solicitação, pela ANPD, do relatório de impacto à proteção de dados pessoais; é interessante que esse artigo trata da não aplicabilidade da Lei a alguns tipos de tratamento de dados pessoais, como aqueles realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais¹⁴, e mesmo diante dessa inaplicabilidade, é dever da Autoridade Nacional emitir opiniões técnicas e recomendações acerca dessas exceções, também solicitar aos responsáveis pelo tratamento a elaboração do relatório de impacto.

Essa previsão demonstra que os agentes de tratamento devem ter cautela em todos os tipos de tratamento de dados pessoais, inclusive naqueles que são exceções e não estão sob a abrangência da legislação, visto que a excepcionalidade não eximirá o controlador da obrigação

¹² “É importante que o RIPD seja entendido não só como uma obrigação, nas circunstâncias apontadas, mas também como um instrumento útil para a avaliação de impactos em qualquer operação de tratamento de dados de forma a contribuir com a mudança cultural corporativa em termos de proteção de dados pessoais e não somente jurídica.” (BORELLI *et al.*, 2020, p. 130).

¹³ Artigo 4º, § 3º da LGPD: “A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.”

¹⁴ Ver artigo 4º, III da LGPD.

de apresentar o relatório de impacto, caso as operações de tratamento requeiram a sua elaboração.

O § 1º desse mesmo artigo deixa claro que os tratamentos de dados não submetidos à aplicação da LGPD devem, ainda assim, observar os princípios gerais de proteção e os direitos do titular previstos na lei. Para Cots e Oliveira¹⁵, foram estabelecidas algumas restrições para o tratamento de dados pelo poder público, pois os bancos de dados públicos passaram a ter alto valor econômico, sendo necessário o estabelecimento de medidas capazes de coibir tentativas de corrupção pelos funcionários públicos ordinários e pelos políticos em geral, chefes do Executivo e Legislativo.

Borelli *et al.*¹⁶ menciona que o caso “Edward Snowden” mostrou que há perigo quando dados coletados para determinada finalidade são utilizados para outros desígnios; então, seria considerada uma medida de boas práticas a elaboração do relatório de impacto pelo poder público, por descrever os processos de tratamento que podem gerar riscos aos direitos fundamentais, também por possibilitar a análise de riscos e a verificação da necessidade e proporcionalidade da coleta dos dados pessoais para atingir a finalidade pretendida.

O relatório é um documento necessário para a descrição dos processos de tratamento de dados pessoais que possuem maiores chances de riscos às liberdades civis e aos direitos fundamentais¹⁷, focando na criação de medidas, salvaguardas e mecanismos de mitigação de riscos. Apesar de a elaboração do relatório de impacto à proteção de dados pessoais pelos controladores não ser obrigatória para todos os tipos de tratamentos de dados, a sua utilização para vários processos trará uma mudança de cultura¹⁸ e fará parte da demonstração da adequação das organizações à LGPD.

O artigo 5º, inciso XVII da Lei apresenta duas definições importantes sobre o RIPD. A primeira é que ele é um documento que contempla os dados, que ao serem tratados, geram alto risco às liberdades civis e aos direitos fundamentais e a segunda é que ele deve conter mecanismos de mitigação de risco.

¹⁵ COTS, Marcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 3. ed. São Paulo: Thomson Reuters, 2020. 263 p.

¹⁶ BORELLI, Alessandra *et al.* Comentários ao GDPR: regulamento geral de proteção de dados da união europeia. 2. ed. São Paulo: Thomson Reuters, 2020. 250 p. Coordenação de Viviane Nóbrega Maldonado e Renato Opice Blum.

¹⁷ Artigo 5º, XVII da LGPD: “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;”

¹⁸ “Necessário destacar a mudança de cultura não somente jurídica, mas corporativa, na medida em que, muito embora a AIPD seja obrigatória somente em alguns casos, ainda assim, isso não significa que esse procedimento não possa ser útil nas demais situações em que se torne mera faculdade.” (BORELLI *et al.*, 2020, p.182).

Conforme explicitado por Borelli et al.¹⁹, a incorporação do RIPD dentro dos procedimentos de governança está totalmente ligada à aplicação dos princípios²⁰ trazidos pela Lei Geral de Proteção de Dados. Por ter a finalidade de mitigar riscos e por não ter um fim em si mesmo, o relatório deve ser elaborado antes mesmo do início do tratamento de dados pessoais²¹. Trata-se de uma ferramenta altamente sofisticada, que analisa possíveis consequências, apresenta orientações sobre o que deve ou não ser feito pelo controlador, a partir da descrição dos tipos dados coletados e da metodologia utilizada.

O relatório de impacto é citado em um terceiro momento na LGPD, em seu artigo 10, §3º²², quando há exposição sobre a possibilidade de a ANPD solicitá-lo ao controlador se houver tratamento de dados cuja base legal utilizada é o legítimo interesse, nos termos do artigo 7º, IX e do artigo 10, I e II.²³ É importante ressaltar que não será necessário elaborar o relatório de impacto para todas as operações de tratamento que envolvam essa base legal, visto que a análise tem como ponto focal os riscos efetivos envolvidos no processo. Por exemplo, no caso dos *cookies* de segurança, mesmo a base legal sendo o legítimo interesse, não seria necessário elaborar um relatório, visto que a atividade é de baixo risco.

Verifica-se, então, que a análise deve ser contextual e que a base legal do legítimo interesse não é a única que enseja a necessidade de elaboração do documento. O consentimento dado pelo titular de dados em um hospital pode significar, por exemplo, uma operação de tratamento que envolve alto risco, gerando a necessidade de elaboração do relatório de impacto, mesmo quando a base legal não é a do legítimo interesse.

¹⁹ BORELLI, Alessandra et al. LGPD: Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters, 2020. 427 p. Coordenação de Viviane Nóbrega Maldonado e Renato Opice Blum.

²⁰ São encontrados dez princípios no Art. 6º da LGPD: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

²¹ “Como o RIPD tem o propósito de mitigar riscos, ele deverá ser realizado antes do início do tratamento, mas com uma visão completa de todo o ciclo de vida dos dados. Assim o controlador conseguirá enxergar, claramente, quais serão os principais fatores que poderão impactar as liberdades civis e os direitos fundamentais para a tomada de decisão, desde a implementação de medidas e mecanismos que demonstrem o cumprimento da Lei até a descontinuidade do projeto.” (BORELLI et al., 2020, p. 127)

²² Artigo 10, § 3º da LGPD: “A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.”

²³ Conforme o Art. 7º, IX da LGPD: “quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”. Conforme o Art. 10, I e II da LGPD: O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Em um quarto momento, ao dispor especificamente sobre o tratamento de dados pessoais pelo poder público, a LGPD prevê, em seu artigo 32,²⁴ que a ANPD poderá solicitar aos agentes do poder público a publicação de relatórios de impacto à proteção de dados pessoais. Consta-se, então, que o relatório poderá ser solicitado quando houver tratamento de dados pessoais pelo poder público, tanto nas operações que estão submetidas à LGPD, quanto nas que são consideradas excepcionais.

É importante ressaltar que há divergência doutrinária em relação à obrigatoriedade de elaboração do relatório de impacto pelo poder público. Borelli et al. entende que é facultativa²⁵ a elaboração do relatório e Cots e Oliveira entende que os entes públicos devem²⁶ elaborar o relatório, visto que a possibilidade de solicitação de sua publicação pressupõe a sua existência.

Como a elaboração do relatório de impacto está relacionada à análise de riscos, é razoável a exigência de sua elaboração ao poder público, assim como ocorre com os demais agentes de tratamento descritos na LGPD, quando o tratamento de dados gerar riscos aos direitos fundamentais dos indivíduos. Outro ponto a ser analisado é que, se o Art. 4º, §3º prevê que a ANPD deverá solicitar relatórios de impacto à proteção de dados pessoais em relação às operações de tratamento descritas no inciso III, em que não há aplicação da lei, não há razões para que ela não solicite também para as operações de tratamento realizadas pelo poder público que estão sujeitas à LGPD.

Há menção também no artigo 38²⁷, que faz parte do Capítulo VI, o qual trata dos agentes de tratamento de dados. Como não há um capítulo específico sobre o relatório de impacto e as disposições sobre o tema estão dispersas na lei, o artigo citado torna-se importantíssimo para o presente estudo, pois é o único que aponta os elementos mínimos²⁸ necessários para a elaboração do relatório, sendo eles a descrição dos tipos de dados coletados, a metodologia

²⁴ Artigo 32 da LGPD: “A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.”

²⁵ “Ao prever, em seu artigo 38, que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto, a interpretação sistemática da LGPD resulta na mera facultatividade de elaborar o RIPDP, imposta ao poder público.” (BORELLI et al., 2020, p. 289)

²⁶ “Assim, entendemos que os entes públicos são obrigados à elaboração do referido relatório, ainda que não o torne público, aguardando deliberação da autoridade.” (COTS; OLIVEIRA, 2020, p. 159)

²⁷ Artigo 38 da LGPD: “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.”

²⁸ Quando a Lei fala sobre requisitos mínimos, entendemos que o rol é exemplificativo e não exaustivo.

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.

Além da possibilidade de solicitação do documento aos controladores e não aos operadores de dados, depreende-se, a partir da análise desse artigo, que um dos objetivos da elaboração do documento é verificar se houve boa-fé e adoção de boas práticas pelo controlador, para que a ANPD possa determinar a sanção a ser aplicada, caso o titular sofra algum dano.

O sexto e último momento em que a LGPD menciona o relatório de impacto é no artigo 55²⁹, em que há descrição das atividades que competem à ANPD, sendo que uma delas é a elaboração de regulamentos e procedimentos sobre relatórios de impacto quando o tratamento apresentar alto risco aos princípios de proteção de dados. A esse respeito, Cots e Oliveira pontuam que é muito difícil³⁰ para o legislador alcançar os detalhes práticos que envolvem o tratamento de dados pessoais, por envolverem ciências e técnicas fora do seu domínio, então cabe à Administração Pública regulamentar as temáticas complexas.

A ANPD já iniciou as movimentações para a elaboração de instruções sobre o relatório de impacto à proteção de dados, visto que abriu um processo de consulta pública de especialistas, a fim de que todos os setores da sociedade pudessem colaborar com as diretrizes desse documento que é imprescindível para a proteção de dados. Durante as reuniões técnicas³¹ houve convergência em relação à interpretação de que a LGPD oferece uma abordagem baseada em riscos. Já houve a publicação do guia orientativo³² para definições dos agentes de tratamento de dados pessoais e do encarregado pela ANPD, e nesse documento o órgão reitera a definição legal do controlador e a sua importância prática no tocante à elaboração do relatório de impacto.

²⁹ Artigo 55, J, XIII da LGPD: “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;”

³⁰ COTS, Marcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 3. ed. São Paulo: Thomson Reuters, 2020. 263 p.

³¹ GARROTE, Marina Gonçalves et al. ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais: análise dos primeiros movimentos da autoridade nacional de proteção de dados. Análise dos primeiros movimentos da Autoridade Nacional de Proteção de Dados. 2021. Disponível em: www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 13 jul. 2021.

³² O guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado dispõe que: “O conceito possui elevada importância prática, uma vez que a LGPD atribui obrigações específicas ao controlador, como a de elaborar relatório de impacto à proteção de dados pessoais (art. 38), a de comprovar que o consentimento obtido do titular atende às exigências legais (art. 8º, § 2º) e a de comunicar à ANPD a ocorrência de incidentes de segurança (art. 48) [...]”

Apesar de existirem diferentes interpretações sobre o documento, há concordância de que ele tem a função de demonstrar para a autoridade de proteção de dados que o tratamento está em *compliance* ou conformidade com a Lei, e que todas as medidas de segurança foram adotadas.

2.2. A ELABORAÇÃO DO RELATÓRIO DE IMPACTO

Como na Lei Geral de Proteção de Dados não há instruções técnicas para elaboração do relatório de impacto, existe uma grande expectativa sobre as regulamentações da ANPD acerca do tema. O órgão divulgou em junho de 2021 o cronograma de reuniões técnicas sobre o relatório de impacto, que aconteceram naquele mesmo mês e foram transmitidas pelo canal da ANPD no Youtube.

Garrote et al.³³ menciona alguns pontos importantes que foram discutidos durante os encontros técnicos da ANPD sobre o relatório de impacto, como a falta de detalhamento na LGPD sobre definições de riscos, a não utilização do porte de uma empresa como parâmetro para definição de alto risco e da obrigatoriedade de elaboração do relatório, a discricionariedade da ANPD para elaboração de *blacklists* e *whitelists*.

O cronograma disponibilizado³⁴ pela ANPD contém os temas que foram discutidos nas reuniões técnicas, os quais foram divididos em três blocos:

³³ GARROTE, Marina Gonçalves *et al.* ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais: análise dos primeiros movimentos da autoridade nacional de proteção de dados. Análise dos primeiros movimentos da Autoridade Nacional de Proteção de Dados. 2021. Disponível em: www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 13 jul. 2021.

³⁴ GOV.BR. ANPD divulga cronograma completo de reuniões técnicas sobre relatório de impacto à proteção dos dados pessoais. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-cronograma-completo-de-reunioes-tecnica>. Acesso em: 07 set. 2021.

Tabela 1 - Cronograma da ANPD sobre as reuniões técnicas

BLOCO 1 - Metodologias e critérios para elaboração e análise do relatório de impacto	1) Existe metodologia recomendada para elaboração do RIPD? Qual? 2) Quais são os elementos que devem constar em um RIPD? 3) Como a ANPD deverá avaliar um RIPD apresentado pelo agente de tratamento? 4) Qual seria um prazo razoável para o agente de tratamento apresentar a ANPD o relatório de impacto de proteção de dados quando solicitado? Deve ser prevista alguma exceção quanto a esse prazo? 5) Existe a possibilidade de a ANPD solicitar a análise prévia do RIPD por auditoria independente? Se sim, em quais casos?
BLOCO 2 - Situações/circunstâncias que ensejam a necessidade ou dispensa de elaboração de relatório de impacto	1) De quem a ANPD deverá solicitar a elaboração do RIPD? Quais são as exceções? 2) Quais são as circunstâncias que devem estar presentes para que um RIPD seja recomendável? Há alguma hipótese em que o relatório de impacto de proteção de dados deveria ser obrigatório? Se sim, qual(is)? E quando ele pode ser dispensado? 3) Essas circunstâncias devem ser as mesmas consideradas para fins de cumprimento da obrigação do art. 4º, §3º, da LGPD? Se não, quais aspectos devem ser considerados? 4) Seria possível a criação de um rol taxativo de obrigatoriedade de elaboração do RIPD? E a criação de um rol taxativo de dispensa?
BLOCO 3 - Transparência e publicidade dos relatórios de impacto para o setor público e o setor privado	1) Em que circunstâncias um tratamento com base no legítimo interesse deve ter por exigência um RIPD prévio? (Art. 10, §3º, da LGPD) Alternativamente, uma Avaliação de Legítimo Interesse não seria suficiente? 2) A publicação de um RIPD pelo poder público deve ser feita em sua íntegra? (Art. 32 da LGPD) Por quê? Caso negativo, quais são os elementos que devem ser publicados e quais devem ser retirados da versão pública? 3) De que maneira o segredo comercial ou industrial poderá limitar o conteúdo de um RIPD? 4) Observados os segredos comerciais e industriais, deveria ser possível solicitar que o setor privado publique o RIPD? Se sim, em quais casos?

A ANPD ainda não regulamentou o tema, então não é possível afirmar qual será a metodologia escolhida pelo órgão; há apenas um indício de que ela seguirá o modelo europeu³⁵, e adotará a metodologia baseada em riscos, a partir da avaliação de impacto feita por meio de critérios objetivos.

³⁵ A própria criação da LGPD foi inspirada no GDPR, então é possível que o órgão siga essa tendência ao regulamentar os pontos específicos da LGPD, como o relatório de impacto.

Descrever as etapas de elaboração de um RIPD não é uma tarefa fácil, devido à sua complexidade prática e à necessidade de adequação regulatória pela Autoridade Nacional de Proteção de Dados. Conforme escrito por Gomes³⁶ muitos setores ainda não compreenderam as funções do relatório e o utilizam para avaliar o nível de conformidade de uma organização com a LGPD.

Entretanto, é importante deixar claro que existem diferenças entre o relatório de diagnóstico e o relatório de impacto, visto que o primeiro é utilizado para gerar um plano de ação para mitigação de riscos e o segundo possui a função de prevenir e mitigar riscos aos direitos dos titulares, com abordagem baseada em direitos e nos riscos regulatórios, também analisa uma operação ou conjunto de operações específicas que podem gerar riscos aos direitos dos titulares.

O relatório de impacto também não pode ser confundido com o teste de legítimo interesse, pois esses documentos possuem funções diferentes. É provável que muitas organizações cometam esse equívoco na prática, porque a LGPD em nenhum momento menciona o teste de legítimo interesse, porém menciona o relatório de impacto em seu artigo 10, §3º.

Antes de elaborar um relatório de impacto, é interessante que seja feita uma avaliação de impacto, para verificar se a operação de tratamento pode gerar impactos graves às liberdades civis e aos direitos fundamentais, e até mesmo para confirmar a necessidade de elaboração do documento, que possui alta complexidade.

Braz Junior³⁷, ao escrever sobre as etapas de elaboração do relatório de impacto, assinala que o propósito não é eliminar todos os riscos, mas minimizar a existência deles e verificar se os riscos remanescentes são justificáveis. Para ele o documento, além de ser uma forma de prestação de contas³⁸ pelos agentes de tratamento, traz benefícios ao negócio à medida em que é capaz de proporcionar a revisão de processos internos.

³⁶ GOMES, Maria Cecília Oliveira. LGPD: desafios da regulamentação do relatório de impacto: anpd publicou portaria que tornou pública a sua agenda regulatória para o biênio 2021 - 2022. ANPD publicou portaria que tornou pública a sua agenda regulatória para o biênio 2021 - 2022. 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: 07 set. 2021.

³⁷ BRAZ JUNIOR, Marcilio. Das etapas de elaboração de um DPIA: propósito de um data protection impact assessment não é eliminar todos os riscos, mas minimizar a existência destes. Propósito de um Data Protection Impact Assessment não é eliminar todos os riscos, mas minimizar a existência destes. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/das-etapas-de-elaboracao-de-um-dpia-27042019>. Acesso em: 27 maio 2021.

³⁸ Um dos princípios da LGPD, descrito no artigo 6º, X é o da responsabilização e prestação de contas.

Ele menciona também as três etapas, que considera essenciais para a elaboração do RIPD; a primeira seria o entendimento da organização e dos processos envolvidos, a partir da realização do mapeamento de dados, que é uma das etapas essenciais para qualquer programa de adequação à LGPD e representa a consolidação de todas as informações referentes ao mapeamento dos processos, subprocessos e das atividades realizadas por determinada organização; as outras duas etapas seriam a avaliação e gerenciamento de riscos.

A partir disso, constatou-se que não seria eficaz a elaboração do relatório de impacto no início de um programa de adequação à LGPD, pois só é possível realizar uma análise completa dos riscos após o mapeamento de dados e consolidação das informações.

2.3. DECISÕES BRASILEIRAS SOBRE O TEMA

O Ministério Público do Distrito Federal e Territórios (MPDFT) instaurou inquérito civil público³⁹ em setembro de 2018 para investigar a legalidade dos serviços oferecidos pela empresa pernambucana In Loco Media, uma startup que desenvolveu um sistema de geolocalização de ambientes internos e externos, que foi explorado por 200 companhias no Brasil.

Na portaria n. 16/2018, o MPDFT considerou o disposto no artigo 5º, X⁴⁰ da Constituição Federal, o Marco Civil da Internet, o Código de Defesa do Consumidor e a LGPD, e entendeu que os fatos eram graves, devido ao vasto número de titulares de dados pessoais afetados, então exigiu a elaboração do relatório de impacto à proteção de dados pessoais.

A empresa In Loco impetrou mandado de segurança para suspender o despacho ministerial que requisitou o relatório de impacto à proteção de dados pessoais, alegando que não caberia ao MPDFT solicitar o documento, mas à ANPD. Na época a LGPD ainda não estava em vigor, portanto foi gerada uma discussão se outros órgão poderiam solicitar a elaboração do relatório, devido à sua especificidade.

Em 2020 a comissão de proteção de dados pessoais do MPDFT arquivou o inquérito de 2018, concluindo que a In Loco não trabalhou com *apps* destinados ao público infantil. A empresa cooperou com a investigação do MPDFT, detalhando o software desenvolvido, de

³⁹ A Portaria n.16/2018 pode ser encontrada em: <https://www.internetlab.org.br/wp-content/uploads/2018/09/mpdf-requerimento.pdf>

⁴⁰ Conforme o artigo 5º, X da Constituição Federal: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;”

forma que a conclusão do inquérito foi que a empresa seguia os padrões exigidos pelo Marco Civil da Internet e da Lei Geral de Proteção de Dados.⁴¹

Outro caso emblemático é o da Telefônica Brasil S.A (Vivo), em que o MPDFT instaurou inquérito civil público (08190.005366/18-16) contra a empresa e requisitou⁴² em abril de 2019, a elaboração de relatório de impacto no prazo de 60 dias, em relação ao tratamento de dados usados para o produto “Mídia Geolocalizada” do serviço “Vivo ads”. No despacho ministerial, o MPDFT especificou quais tópicos deveriam constar no relatório de impacto⁴³:

Tabela 2 - Tópicos do despacho ministerial do MPDFT

1 - Como a organização descreve o tratamento de dados realizado
A natureza do tratamento é o que a organização planeja fazer com os dados pessoais. Isso deve incluir:
Como a organização coleta os dados; Como a organização armazena os dados; Como a organização usa os dados; Quem tem acesso aos dados; Com quem são compartilhados os dados; Se a organização utiliza operadores (pessoa natural ou jurídica que realiza o tratamento de dados em nome do operador) para tratar os dados; Períodos de retenção; Medidas de segurança; Se a organização utiliza novas tecnologias, e; Se a organização usa algum tipo novo de tratamento.
O escopo é o que o tratamento abrange. Isso deve incluir:
A natureza dos dados pessoais; O volume e a variedade dos dados pessoais; A sensibilidade dos dados pessoais; A extensão e frequência do tratamento; A duração do tratamento; O número de dados envolvidos, e; A área geográfica coberta.
O contexto do tratamento é um quadro mais amplo, incluindo fatores internos e externos que podem afetar as expectativas ou o impacto. Isso deve incluir:
A fonte dos dados; A natureza do relacionamento da organização com os indivíduos; Até que ponto os indivíduos têm controle sobre seus dados; Até onde os indivíduos provavelmente esperam o tratamento; Se entre os indivíduos incluem-se menores de 18 anos ou outras pessoas vulneráveis; Qualquer experiência anterior com este tipo de tratamento; Quaisquer avanços relevantes em tecnologia ou segurança, e; Quaisquer questões atuais de interesse público.
O objetivo do tratamento é o motivo pelo qual a organização faz o tratamento dos dados. Isso deve incluir:
Seus interesses legítimos, quando relevantes; O resultado pretendido para os indivíduos; Os benefícios esperados para a organização ou para a sociedade como um todo.
2 – Como a organização avalia a necessidade e proporcionalidade do tratamento de dados

⁴¹ LOPES, André. MP arquiva caso de startup que teria rastreado 60 milhões de celulares: a suspeita era de que a empresa conseguia dados de geolocalização sem consentimento dos usuários. A suspeita era de que a empresa conseguia dados de geolocalização sem consentimento dos usuários. 2020. Disponível em: <https://veja.abril.com.br/tecnologia/mp-arquiva-caso-de-startup-que-teria-rastreado-60-milhoes-de-celulares/>. Acesso em: 08 set. 2021.

⁴² O despacho ministerial por ser encontrado em: https://www.mpdft.mp.br/portal/pdf/Despacho_DPIA_3_1.pdf

⁴³ No despacho ministerial do Ministério Público supracitado é possível encontrar os tópicos descritos, os quais foram transformados em tabela pela autora.

Existe alguma outra maneira razoável de alcançar o mesmo resultado; Qual a base legal usada para o tratamento de dados; Como a organização pretende garantir a qualidade dos dados; Como a organização pretende fornecer informações de privacidade para os indivíduos; Medidas adotadas para garantir o cumprimento da legislação e das ordens dadas aos operadores, e; Quais são as salvaguardas para as transferências internacionais de dados.

3 – Como a organização identifica e avalia os riscos

Deve ser considerado o impacto potencial sobre os indivíduos e qualquer dano que seu tratamento possa causar, seja físico, emocional ou material. Em particular, observe se o tratamento poderá contribuir para: Incapacidade de exercer direitos (incluindo, mas não se limitando, a direitos de privacidade); Incapacidade de acessar serviços ou oportunidades; Perda de controle sobre o uso de dados pessoais; Discriminação; Roubo de identidade ou fraude; Perda financeira; Danos à reputação; Danos físicos; Perda de confidencialidade, ou; Qualquer outra desvantagem econômica ou social significativa.

A organização deve incluir uma avaliação dos riscos de segurança, incluindo fontes de risco e o impacto potencial de cada tipo de violação (incluindo acesso ilegítimo, modificação ou perda de dados pessoais).

Para avaliar se o risco é alto, a organização precisa considerar tanto a probabilidade quanto a gravidade do possível dano.

O dano não precisa ser inevitável para se qualificar como risco.

Qualquer possibilidade significativa de danos muito sérios pode ser suficiente para se qualificar como alto risco.

A organização deve se atentar para o fato de que uma alta probabilidade de danos generalizados, ainda que com impactos menores, pode ser igualmente considerada de alto risco.

A organização deve fazer uma avaliação objetiva dos riscos.

É útil usar uma matriz estruturada para pensar sobre a probabilidade e a gravidade dos riscos.

4 – Como a organização identifica e mitiga os riscos

Contra cada risco identificado, registre a fonte.

A organização deve considerar opções para reduzir estes riscos, como por exemplo:

Decidir não coletar certos tipos de dados; Reduzir o escopo do processamento; Reduzir os períodos de retenção; Tomar medidas adicionais de segurança tecnológica; Treinar os colaboradores para garantir que os riscos sejam antecipados e gerenciados; Anonimizar ou pseudoanonimizar os dados, sempre que possível; Elaborar orientações ou processos internos para evitar riscos; Colocar em prática acordos claros de compartilhamento de dados; Fazer alterações nas políticas de privacidade; Implementar novos sistemas para ajudar os indivíduos a exercerem seus direitos.

5 – Conclusão do Relatório de Impacto à Proteção de Dados Pessoais

A Organização deve informar:

Que medidas adicionais pretende adotar; Se cada risco foi eliminado, reduzido ou aceito; O nível global de risco residual, após a adoção de medidas adicionais.

6 – Assinaturas dos Responsáveis pela Elaboração do Relatório de Impacto à Proteção de Dados Pessoais (Encarregado/ Data Protection Officer – DPO ou Diretor da Organização)

O Ministério Público alegou que o serviço da Vivo fornecia publicidade usando dados qualificados dos clientes da operadora, como perfil, localização, navegação, lugares frequentados e comportamento dos consumidores, então solicitou a elaboração do relatório de impacto, a fim de que a empresa pudesse comprovar a legalidade do serviço. Diante da negativa da empresa, o órgão entendeu que o tratamento de dados pessoais era indevido.

Dessa forma, foi ajuizada ação civil pública⁴⁴ em desfavor da Telefônica Brasil S.A. requerendo a sua condenação à obrigação de não fazer, consistente em deixar de comercializar o produto “Mídia geolocalizada do serviço Vivo Ads”, e à obrigação de fazer, para elaboração do relatório de impacto à proteção de dados pessoais, como havia sido requisitado no inquérito civil público. Apesar das alegações do Ministério Público, o juiz de primeira instância julgou os pedidos improcedentes e a turma negou provimento ao recurso.

Assim como no caso da In Loco, houve questionamento sobre a possibilidade de exigência do relatório de impacto antes da regulamentação da ANPD.

3. O RELATÓRIO DE IMPACTO NO GDPR

3.1. A PREVISÃO LEGAL DA AVALIAÇÃO DE IMPACTO NO GDPR

O DPIA⁴⁵ é tratado no GDPR em um capítulo específico, diferentemente da LGPD, que trata do tema de forma esparsa. Seu artigo 35 trata da avaliação de impacto sobre a proteção de dados:

1. Quando certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.
2. Ao efetuar uma avaliação de impacto sobre proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.
3. A realização de uma avaliação de impacto sobre a proteção de dados, a que se refere o n.º 1 é obrigatória nomeadamente em caso de:
 - a) avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
 - b) operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; ou
 - c) controle sistemático de zonas acessíveis ao público em grande escala.

⁴⁴ Consultar processo 0721735-15.2019.8.07.0001 da 24ª Vara Cível de Brasília.

⁴⁵ O DPIA pode ser traduzido como Avaliação de impacto sobre a proteção de dados.

4. A autoridade de controle elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do n.º 1. A autoridade de controle comunica essas listas ao comitê referido no artigo 68º.

5. A autoridade de controle pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados. A autoridade de controle comunica essas listas ao comitê.

6. Antes de adotar as listas a que se referem os n.ºs 4 e 5, a autoridade de controle competente aplica o procedimento de controle da coerência referido no artigo 63.o sempre que essas listas enunciem atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controle do seu comportamento em diversos Estados-Membros, ou possam afetar substancialmente a livre circulação de dados pessoais na União.

7. A avaliação inclui, pelo menos:

- a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
- b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
- c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1; e
- d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

8. Ao avaliar o impacto das operações de tratamento efetuadas pelos responsáveis pelo tratamento ou pelos subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, é tido na devida conta o cumprimento dos códigos de conduta aprovados a que se refere o artigo 40.º por parte desses responsáveis ou subcontratantes.

9. Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento.

10. Se o tratamento efetuado por força do artigo 6.º, n.º 1, alínea c) ou e), tiver por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico, não são aplicáveis os n.ºs 1 a 7, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento.

11. Se necessário, o responsável pelo tratamento procede a um controle para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam.

O artigo 35, 1 do GDPR dispõe que a avaliação de impacto deve ser feita quando o tratamento for suscetível de implicar elevado risco para os direitos e liberdades das pessoas singulares, levando em conta a natureza, o âmbito, o contexto e a finalidade. A inserção na

legislação desses pontos a serem observados demonstra que a análise das operações de tratamento que envolvem dados pessoais deve ser feita de forma contextual, visto que um mesmo dado pessoal pode ser utilizado para diferentes finalidades, que na prática podem acarretar alto risco ao titular de dados ou não.

O responsável pelo tratamento deve realizar a avaliação de impacto antes de iniciar o tratamento e, caso houver um conjunto de operações de tratamento, que apresentem riscos elevados semelhantes, é possível realizar a análise em uma única avaliação, por economia procedimental⁴⁶.

O artigo 35, 2 demonstra que o responsável pelo tratamento, ao efetuar a avaliação de impacto, deve solicitar o parecer do encarregado⁴⁷ de proteção de dados, nos casos em que ele tiver sido designado. Já o 3 explicita que é obrigatória a realização de avaliação de impacto sobre a proteção de dados quando houver avaliação sistêmica de aspectos pessoais baseada no tratamento automatizado, quando ocorrer tratamento de categorias especiais⁴⁸ de dados pessoais em grande escala ou relacionados com condenações penais e infrações⁴⁹ e quando houver controle sistemático de zonas acessíveis ao público em grande escala.

O artigo 35, nº 4, 5 e 6 tratam da competência da autoridade para elaboração e publicação de listas dos tipos de operações de tratamento que estão sujeitos ou não à avaliação de impacto.

O artigo 35, nº 7 anuncia que a avaliação deve conter pelo menos a descrição das operações de tratamento, a finalidade, se for o caso os interesses legítimos do responsável pelo tratamento, a avaliação da necessidade e proporcionalidade do tratamento em relação aos objetivos, uma avaliação dos riscos para os direitos e liberdades dos titulares e as medidas a serem tomadas frente aos riscos; no nº 8 há menção sobre a necessidade de cumprimento dos códigos de conduta aprovados⁵⁰, por parte dos responsáveis ou subcontratantes.

⁴⁶ PINHEIRO, Alexandre Sousa *et al.* Comentário ao Regulamento Geral de Proteção de Dados. Coimbra: Almedina, 2018. 709 p.

⁴⁷ O artigo 39, 1, c do GDPR diz que: “O encarregado da proteção de dados tem, pelo menos, as seguintes funções: (...) Presta aconselhamento quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção da dados e controla a sua realização nos termos do artigo 35º;”

⁴⁸ Conforme artigo 9º, 1 do GDPR: “É proibido o tratamento de dados pessoais que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.”

⁴⁹ Conforme artigo 10º do GDPR: “O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.º, n.º 1, só é efetuado sob o controle de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas.

⁵⁰ Conforme artigo 40º do GDPR.

O artigo 35, n.º 9, está relacionado ao princípio da proporcionalidade em sentido amplo, na sua dimensão de adequação, quando há possibilidade de os responsáveis pelo tratamento solicitarem a opinião dos titulares de dados ou seus representantes, sem prejuízos aos interesses comerciais ou públicos ou da segurança da operação de tratamento.

Por fim, o n.º 10 prevê a possibilidade de não aplicação⁵¹ dos n.ºs 1 a 7 do presente artigo, ao passo que o n.º 11 prevê que o responsável pelo tratamento poderá, se necessário, avaliar se o tratamento realizado está em conformidade com a avaliação de impacto sobre a proteção de dados pessoais, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam.

O artigo 36 do GDPR trata sobre a consulta prévia à autoridade de controle:

1. O responsável pelo tratamento consulta a autoridade de controle antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.
2. Sempre que considerar que o tratamento previsto referido no n.º 1 violaria o disposto no presente regulamento, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controle, no prazo máximo de oito semanas a contar da recepção do pedido de consulta, dá orientações, por escrito, ao responsável pelo tratamento e, se o houver, ao subcontratante e pode recorrer a todos os seus poderes referidos no artigo 58.o. Esse prazo pode ser prorrogado até seis semanas, tendo em conta a complexidade do tratamento previsto. A autoridade de controle informa da prorrogação o responsável pelo tratamento ou, se o houver, o subcontratante no prazo de um mês a contar da data de recepção do pedido de consulta, juntamente com os motivos do atraso. Esses prazos podem ser suspensos até que a autoridade de controle tenha obtido as informações que tenha solicitado para efeitos da consulta.
3. Quando consultar a autoridade de controle nos termos do n.º 1, o responsável pelo tratamento comunica-lhe os seguintes elementos:
 - a) Se for aplicável, a repartição de responsabilidades entre o responsável pelo tratamento, os responsáveis conjuntos pelo tratamento e os subcontratantes envolvidos no tratamento, nomeadamente no caso de um tratamento dentro de um grupo empresarial;
 - b) As finalidades e os meios do tratamento previsto;
 - c) As medidas e garantias previstas para defesa dos direitos e liberdades dos titulares dos dados nos termos do presente regulamento;
 - d) Se for aplicável, os contatos do encarregado da proteção de dados;

⁵¹ “O n.º 10 prevê a desaplicação dos n.ºs 1 ao 7 do presente artigo, mediante a verificação dos seguintes pressupostos: (i) se o tratamento efetuado for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito ou para o exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido tiver por fundamento jurídico o direito da União ou do Estado-Membro a que esteja sujeito, (ii) esse direito regular a operação ou as operações de tratamento específicas em questão, (iii) prévia realização de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico e (iv) os Estados-Membros considerarem desnecessário proceder a essa avaliação antes das atividades de tratamento.” (PINHEIRO *et al.*, 2018, p. 462)

- e) A avaliação de impacto sobre a proteção de dados prevista no artigo 35.º; e
- f) Quaisquer outras informações solicitadas pela autoridade de controle.

4. Os Estados-Membros consultam a autoridade de controle durante a preparação de uma proposta de medida legislativa a adotar por um parlamento nacional ou de uma medida regulamentar baseada nessa medida legislativa, que esteja relacionada com o tratamento de dados.

5. Não obstante o n.º 1, o direito dos Estados-Membros pode exigir que os responsáveis pelo tratamento consultem a autoridade de controle e dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública.

A partir da análise desse artigo, fica evidente a complexidade de uma avaliação de impacto à proteção de dados, pois a autoridade possui prazo de oito semanas, o qual pode ser prorrogado por mais seis semanas, para orientar o responsável pelo tratamento em sua solicitação de orientação. Além das organizações privadas, os Estados-Membros também consultam a autoridade quando estiverem elaborando medida legislativa ou medida regulamentar que envolva o tratamento de dados.

Os “considerandos” presentes do GDPR também devem ser analisados, à medida em que podem auxiliar na compreensão dos artigos 35 e 36 da legislação, os quais dispõem especificamente sobre a avaliação de impacto à proteção de dados. É importante destacar os “considerandos” 75, 84, 89, 90, 91, 92 e 93, que falam respectivamente sobre:

- a) os riscos para os direitos e liberdades que podem gerar danos aos titulares;
- b) a necessidade de realização da avaliação de impacto e levantamento de medidas comprobatórias sobre a conformidade da operação de tratamento ao regulamento;
- c) a supressão e substituição do previsto na Diretiva 95/46/CE por regras e procedimentos eficazes focados nas operações de tratamento que podem gerar elevado risco para os direitos e liberdades das pessoas;
- d) a necessidade de elaboração da avaliação de impacto para avaliar a probabilidade ou gravidade do elevado risco;
- e) os casos em que é necessário fazer a avaliação de impacto;
- f) a possibilidade de alargar a avaliação de impacto para além de um projeto único;
- g) proceder à avaliação de impacto antes do início das atividades de tratamento pelos Estados-Membros.

3.2. A ELABORAÇÃO DA AVALIAÇÃO DE IMPACTO

A comissão europeia de proteção de dados diz que o DPIA deve ser elaborado quando o tratamento de dados pode gerar alto risco aos direitos e liberdades individuais. É necessária a elaboração da avaliação de impacto, quando houver:

- i. avaliação sistemática e extensiva dos aspectos pessoais relativos às pessoas singulares com base no tratamento automatizado;
- ii. tratamento em grande escala de categorias especiais de dados a que se refere o artigo 10 ou dados relativos a condenações penais e infrações a que se refere o artigo 11;
- iii. monitoramento sistemático de uma área acessível ao público em grande escala;

Se a atividade de tratamento não se referir a um dos itens listados acima, os quais não são exaustivos, o controlador deverá avaliar se há necessidade de elaboração de um DPIA, respondendo às perguntas do documento de avaliação de impacto.⁵²

Tabela 3 - Modelo do EDPS para avaliação de impacto.

Critérios	Sim	Não
Avaliação sistemática e extensa de aspectos pessoais ou pontuação, incluindo criação de perfil e previsão;		
Tomada de decisão automatizada com efeito legal ou significativo;		
Monitoramento sistemático: processamento utilizado para observar, monitorar ou controlar os titulares de dados, especialmente em locais acessíveis ao público;		
Dados sensíveis ou de natureza altamente pessoal;		
Dados processados em grande escala;		
Conjunto de dados combinados a partir de diferentes operações de processamento de dados realizadas para diferentes fins;		

⁵² EDPS. Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments. 2019. Disponível em: https://edps.europa.eu/sites/edp/files/publication/19-0717_accountability_on_the_ground_part_i_en.pdf. Acesso em: 18 set. 2021.

Dados relativos a titulares vulneráveis;		
Uso inovador ou aplicação de soluções tecnológicas ou organizacionais que podem envolver novas formas de tratamento;		
Impedir que os titulares dos dados exerçam um direito ou usem um serviço ou contrato;		

Se forem marcados dois ou mais “sim” é necessário elaborar o relatório; se no caso concreto, for constatado que, mesmo sendo marcado dois ou mais “sim”, os riscos não são altos, é necessário explicar e justificar o motivo do tratamento não ser considerado de alto risco.

Segundo a comissão, as autoridades nacionais de proteção de dados, em conformidade com as orientações da *European Data protection supervisor* (EDPS), podem elaborar listas de casos em que é necessário realizar um DPIA. Esse documento deve ser elaborado antes do início do tratamento de dados e deve ser considerado uma ferramenta viva.

Eles mencionam, por exemplo, que um médico que trata dados de seus pacientes não precisa elaborar um DPIA, desde que esse tratamento não seja feito em larga escala e que o número de pacientes seja limitado. Já um hospital que pretenda implementar um novo banco de dados com informações de saúde, que contenha informações dos pacientes, deve elaborar um DPIA.

O órgão ressalta que a elaboração da avaliação de impacto é uma das formas de *accountability*, que é a capacidade do controlador de dados em demonstrar conformidade com a legislação.

3.3. DECISÕES EUROPEIAS SOBRE O TEMA

Em agosto de 2020 a suprema corte do Reino Unido julgou o caso “Edward Bridges x The Chief Constable of South Wales Police”. O tribunal concluiu que o uso de tecnologia de reconhecimento facial automatizado pela polícia do País de Gales era ilegal e não estava em conformidade com o artigo 8 da convenção europeia sobre direitos humanos.

O caso foi apresentado por Edward Bridges, um ativista das liberdades civis que mora em Cardiff. Ele contestava a legalidade da tecnologia de reconhecimento facial automatizado, que havia sido implementada pela polícia de Gales para identificar pessoas procuradas; quando

a tecnologia identificava uma possível correspondência, as imagens eram analisadas por um operador da tecnologia para confirmação.

Em um primeiro momento foi decidido que a tecnologia era necessária e não operava de forma discriminatória, entretanto Bridges recorreu da decisão, alegando que o tribunal errou ao sustentar que a avaliação de impacto à proteção de dados, elaborada pela polícia de Gales, estava em conformidade com a legislação. Dos cinco pontos contestados em seu recurso, Bridges teve sucesso em três, dentre eles o que mencionava o DPIA.

4. COMPARATIVO ENTRE A PREVISÃO EUROPEIA E A BRASILEIRA

A metodologia utilizada no presente estudo comparado é a funcionalista moderada, que se difere do método funcional tradicional, o qual analisa somente as semelhanças entre os ordenamentos jurídicos, visto que é uma tentativa contemporânea de uma variante nova e moderada do método funcional, que leva em consideração tanto as semelhanças quanto as diferenças entre os ordenamentos jurídicos e pressupõe uma decisão sobre o enfoque da comparação somente após a pesquisa concreta dos ordenamentos.

Como a metodologia de comparação adotada foi a funcional moderada, houve a análise prévia das disposições legais acerca do relatório de impacto nas legislações brasileiras e europeias, bem como das decisões envolvendo o tema, para que, assim, fosse possível estruturar as semelhanças e diferenças existentes entre os ordenamentos jurídicos.

A primeira diferença relevante entre as legislações é que no GDPR há um capítulo específico sobre o relatório de impacto, porém na LGPD o tema está disperso entre os capítulos. No capítulo que trata das disposições preliminares há disposição no sentido de que a ANPD deverá solicitar relatórios de impacto em relação às exceções previstas no inciso III do artigo 4º e há também a definição de relatório de impacto no artigo 5º, XVII.

Já no capítulo intitulado “Do tratamento de dados pessoais”, especificamente no artigo 10, que fala sobre a base legal do legítimo interesse, há menção sobre a possibilidade de a ANPD solicitar a elaboração do relatório de impacto. No capítulo que trata “Do tratamento de dados pessoais pelo poder público” a lei fala que a ANPD poderá solicitar, aos agentes do poder publico, a publicação do relatório de impacto.

No capítulo “Dos agentes de tratamento de dados pessoais”, no artigo 38, a lei traz os requisitos mínimos que devem conter no relatório de impacto e, por fim, no artigo 55J, dentro do capítulo “Da autoridade nacional de proteção de dados (ANPD) e do conselho nacional de

proteção de dados pessoais e da privacidade”, o legislador fala sobre a responsabilidade da ANPD na edição de regulamentos sobre o relatório de impacto.

Observa-se, então, que a maior parte das menções sobre o relatório de impacto à proteção de dados pessoais referem-se ao dever ou possibilidade de a ANPD solicitar a elaboração do documento e a menor parte demonstra as definições e requisitos mínimos necessários.

Ao revés do que ocorre na LGPD, no GDPR há um capítulo denominado *Data protection impact assessment and prior consultation*, dedicado às exposições específicas sobre o DPIA, nos artigos 35 e 36. É possível encontrar nesses artigos as definições, a indicação da pessoa responsável pelo documento, o momento indicado para a elaboração, os casos em que é obrigatória a elaboração do relatório de impacto, os papéis das autoridades de proteção de dados, entre outros.

Outra diferença observada na análise das duas legislações é a especificação do momento em que o relatório deve ser elaborado. No GDPR há previsão, no artigo 35, 1, de que o relatório de impacto deve ser realizado antes do início do tratamento, porém na LGPD não é possível encontrar disposições nesse sentido. É importante destacar que no GDPR há definição do que seria um tratamento de dados pessoais de alto risco e das atividades que ensejam a obrigatoriedade de elaboração do relatório de impacto, ao contrário da LGPD que apenas menciona a necessidade de elaborar o documento quando os processos de tratamento podem gerar riscos às liberdades civis e aos direitos fundamentais, sem especificar quais seriam esses tratamentos de alto risco.

No GDPR, o responsável pelo tratamento deve solicitar o parecer do encarregado de proteção de dados, quando ele tiver sido designado, também poderá solicitar a opinião dos titulares de dados, quando for adequado. Na LGPD não há menção sobre essas questões acima descritas.

Quanto às semelhanças, as duas legislações trazem os procedimentos para elaboração do relatório de impacto. O GDPR informa que a avaliação de impacto deve possuir, pelo menos, a descrição, a finalidade, a necessidade e a proporcionalidade do tratamento, também uma avaliação de riscos para direitos e liberdades dos titulares e as medidas a serem tomadas frente aos riscos, como forma de demonstração de conformidade com a lei.

A partir da análise do artigo 38 da LGPD, depreende-se apenas que o relatório de impacto deve 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. Diante disso, fica claro que a descrição desses procedimentos é mais completa no GDPR.

Outro ponto é que, tanto a LGPD quanto o GDPR trazem previsões sobre o papel das autoridades nacionais na regulamentação do tema nos países, ocorre que na LGPD há apenas a descrição dos momentos em que a ANPD poderá solicitar o RIPD e a sua responsabilidade em regulamentar a matéria, já no GDPR existe uma orientação mais completa, de que o responsável pelo tratamento de dados pessoais deverá consultar a autoridade nacional antes de iniciar o tratamento quando houver elevado risco, da possibilidade de a autoridade elaborar e tornar públicas listas das operações de tratamento indicando quando é necessário e quando não é necessário elaborar o relatório de impacto.

Quanto ao processo prático de elaboração do relatório de impacto, já houve na Europa regulamentação do tema pelo EDPS, porém no Brasil a ANPD ainda está em processo de análise do tema. É muito provável que as orientações do órgão brasileiro sejam semelhantes às do órgão europeu, visto que a própria redação da legislação brasileira teve inspirações no GDPR.

Tabela 4 - Tabela comparativa sobre o relatório de impacto

CARACTERÍSTICAS	LGPD	GDPR
Capítulo específico sobre o tema	Não	Sim
Momento da elaboração	Não	Sim
Definição de alto risco	Não	Sim
Solicitação de parecer do encarregado de dados	Não	Sim
Solicitação de opinião do titular de dados	Não	Sim
Procedimentos para elaboração	Sim	Sim
O papel das autoridades nacionais em relação ao tema	Sim	Sim

5. CONSIDERAÇÕES FINAIS

O presente estudo acerca do relatório de impacto à proteção de dados, demonstra a grande relevância do tema, devido à natureza das atividades que ensejam a sua elaboração, as quais são passíveis de gerar riscos às liberdades civis e aos direitos fundamentais dos indivíduos.

Após a pesquisa sobre as disposições legais sobre o relatório de impacto à proteção de dados na LGPD e no GDPR e da análise das decisões que permeiam o tema, foi possível realizar

um estudo comparado, utilizando a metodologia funcional moderada, que possibilita a identificação das semelhanças e diferenças entre as legislações.

A legislação europeia de proteção de dados inspirou outros países, inclusive o Brasil, devido à sua maior maturidade em relação ao assunto. Percebe-se que, no GDPR, o estudo sobre o relatório de impacto é mais detalhado, possuindo um capítulo específico para tratar do tema, bem como os “considerandos”.

O GDPR e a LGPD se assemelham quanto à indicação de procedimentos para elaboração do relatório de impacto, também na indicação do papel da autoridade nacional na regulamentação do tema. As principais diferenças estão relacionadas à existência de capítulo específico para tratar do tema, a indicação do momento adequado para elaborar o documento, a definição de operações de tratamento que indicam alto risco, a solicitação de parecer do encarregado de dados e a solicitação de opinião do titular. É possível concluir, assim, que existem mais diferenças do que semelhanças entre as duas legislações mencionadas.

REFERÊNCIAS

BATSFORD, James; DAUTLICH, Marc; HARRISON, Faye. Lessons learned: **Completing a DPIA for an AI use case**. Disponível em: <https://www.lexology.com/library/detail.aspx?g=c0621860-711b-450e-8e5e-b54f47bb437a>. Acesso em: 30 set. 2021.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. Rio de Janeiro: Zahar, 2014. 159 p. Tradução de Carlos Alberto Medeiros.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. 298 p.

BORELLI, Alessandra et al. **Comentários ao GDPR: regulamento geral de proteção de dados da união europeia**. 2. ed. São Paulo: Thomson Reuters, 2020. 250 p. Coordenação de Viviane Nóbrega Maldonado e Renato Opice Blum.

BORELLI, Alessandra et al. **LGPD: Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters, 2020. 427 p. Coordenação de Viviane Nóbrega Maldonado e Renato Opice Blum.

BRAZ JUNIOR, Marcilio. **Das etapas de elaboração de um DPIA**: propósito de um data protection impact assessment não é eliminar todos os riscos, mas minimizar a existência destes. Propósito de um Data Protection Impact Assessment não é eliminar todos os riscos, mas

minimizar a existência destes. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/das-etapas-de-elaboracao-de-um-dpia-27042019>. Acesso em: 27 maio 2021.

COTS, Marcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada**. 3. ed. São Paulo: Thomson Reuters, 2020. 263 p. DATAPRIVACYBR. **Memória da LGPD**. 2020. Disponível em: <https://www.observatorioprivacidade.com.br/memorias/>. Acesso em: 25 maio 2021.

CURY, Paula Maria Nasser. Métodos de Direito Comparado: desenvolvimento ao longo do século xx e perspectivas contemporâneas. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito**, [S.L.], v. 6, n. 2, p. 176-185, 18 maio 2014. UNISINOS - Universidade do Vale do Rio Dos Sinos. <http://dx.doi.org/10.4013/rechtd.2014.62.06>.

EDPS. **Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments**. 2019. Disponível em: https://edps.europa.eu/sites/edp/files/publication/19-0717_accountability_on_the_ground_part_i_en.pdf. Acesso em: 18 set. 2021.

EDPS. **When is a Data Protection Impact Assessment (DPIA) required?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en. Acesso em: 18 set. 2021.

GARROTE, Marina Gonçalves *et al.* **ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais**: análise dos primeiros movimentos da autoridade nacional de proteção de dados. Análise dos primeiros movimentos da Autoridade Nacional de Proteção de Dados. 2021. Disponível em: www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021. Acesso em: 13 jul. 2021.

GOMES, Maria Cecilia Oliveira. **LGPD: desafios da regulamentação do relatório de impacto**: anpd publicou portaria que tornou pública a sua agenda regulatória para o biênio 2021 - 2022. ANPD publicou portaria que tornou pública a sua agenda regulatória para o biênio 2021 - 2022. 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: 07 set. 2021.

GOV.BR. **ANPD abre inscrições para participação em reunião técnica sobre relatório de impacto de proteção de dados pessoais**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-inscricoes-para-participacao-em-reuniao-tecnica-sobre-relatorio-de-impacto-de-protecao-de-dados-pessoais>. Acesso em: 26 maio 2021.

GOV.BR. **ANPD divulga cronograma completo de reuniões técnicas sobre relatório de impacto à proteção dos dados pessoais**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-cronograma-completo-de-reunioes-tecnica>. Acesso em: 07 set. 2021.

ICO. **Data protection impact assessments**. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments>

DONEDA, Danilo. **Da privacidade à Proteção de Dados Pessoais**: fundamentos da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters, 2020. 352 p.

MONTEIRO, Renato Leite. **GDPR matchup: Brazil's General Data Protection Law**. 2018. Disponível em: <https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/>. Acesso em: 25 maio 2021.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 29 dez. 2018.

LIMA, Adriano Carlos de et al. **LGPD - Lei Geral de Proteção de Dados**: manual de implementação. São Paulo: Thomson Reuters, 2019. 368 p. Coordenação de Viviane Nóbrega Maldonado.

LOPES, André. **MP arquiva caso de startup que teria rastreado 60 milhões de celulares**: a suspeita era de que a empresa conseguia dados de geolocalização sem consentimento dos usuários. A suspeita era de que a empresa conseguia dados de geolocalização sem consentimento dos usuários. 2020. Disponível em: <https://veja.abril.com.br/tecnologia/mp-arquiva-caso-de-startup-que-teria-rastreado-60-milhoes-de-celulares/>. Acesso em: 08 set. 2021.

PINHEIRO, Alexandre Sousa *et al.* **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018. 709 p.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: comentários à lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020. 152 p.

RODOTÀ, Stefano. **A vida na sociedade da Vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. 382 p. Tradução de Danilo Doneda e Luciana Cabral Doneda.

SABBAGH, Dan. **South Wales police lose landmark facial recognition case: call for forces to drop tech use after court ruled it breached privacy and broke equalities law**. Disponível em: <https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recogniti>. Acesso em: 30 set. 2021.