RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS: UMA BANALIZAÇÃO?

PERSONAL DATA PROTECTION IMPACT REPORT (RIPD) IN BRAZILIAN GENERAL DATA PROTECTION LAW: A BANALIZATION?

IAN MATIELLO GRASSO[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. A VIRADA REGULATÓRIA. 3. BREVE HISTÓRICO DAS FERRAMENTAS. 4. CONCLUSÕES. BIBLIOGRAFIA.

RESUMO

Este artigo tem como objetivo estudar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) a partir de seus predecessores: as *impact assessments*, o *Privacy Impact Assessment*, do Reino Unido, e o *Data Protection Impact Assessment (DPIA), do General Data Protection Regulation (GDPR)*, analisando a experiência europeia sobre o tema, bem como de que modo a regulação brasileira o incorporou, explorando possíveis problemas e soluções.

Palavras-chave: Direito Digital; Lei Geral de Proteção de Dados; Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

ABSTRACT

This article aims to study the Personal Data Protection Impact Report (RIPD) from its predecessors: as impact assessments, the UK Privacy Impact Assessment and the Data Protection Impact Assessment (DPIA) of the General Data Protection Regulation (GDPR), analyzing the European experience on the subject, as well as how Brazilian regulation incorporated it, exploring possible problems and solutions.

Keywords: Digital Law; Brazilian General Data Protection Law; Personal Data Protection Impact Report (RIPD).

1 INTRODUÇÃO

[1] Graduando em Direito pela Faculdade de Direito de Sorocaba. Artigo Científico apresentado como resultado dos trabalhos realizados no Grupo de Estudos em Direito Digital da Faculdade de Direito de Sorocaba (2020-2021). E-mail. ian.m.grasso@hotmail.com.

A Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais), em vigor desde 18/09/2020, tornou-se, no ordenamento jurídico pátrio, a peça central na sistemática de proteção aos direitos de privacidade e dos titulares de dados pessoais. A abordagem regulatória trazida pela LGPD é parte de um novo capítulo no mundo jurídico, o da "risquificação" dos direitos, "onde a afirmação de direitos fundamentais é complementada por uma preocupação maior com instrumentos de regulação *ex ante*, licenças, análises de risco, processos de documentação e accountability por parte dos 'controladores' e 'processadores' de dados (GELLERT, 2015; QUELLE, 2015; SPINA, 2017).[2]'

Nesta perspectiva, para operacionalizar seus ditames na rotina das organizações, "a LGPD pode ser encarada como uma 'caixa de ferramentas' (BENNETT; RAAB, 2006), na qual vão existir obrigações que servem como instrumentos e conceitos que nos ensinam a como manusear essas ferramentas de forma adequada e eficiente[3]".

A base teórica da lei geral brasileira foi inspirada fortemente pela experiência europeia de elaboração do *General Data Protection Regulation (GDPR)*, com adaptações pelo legislador nacional, trazendo diversas obrigações e instrumentos semelhantes entre si, e entre eles, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), equivalente ao *Data Protection Impact Assessment (DPIA)* europeu.

A ferramenta foi pensada e moldada com a função de desempenhar papel central na sistemática de proteção de dados do bloco europeu[4]. Assim sendo, "errar a mão" em sua regulação tem duas consequências principais que serão catastróficas: desperdiçará e dissipará os esforços da Autoridade Nacional de Proteção de Dados (ANPD) e onerará excessivamente os controladores e operadores com uma possível obrigação legal meramente formal, o que vai na contramão da sistemática preventiva trazida pelo *GDPR* e pela LGPD.

Até o momento, permanece o cenário de incertezas de como o tema será abordado pela Autoridade Nacional, e os desafios para a regulação do RIPD não são poucos, principalmente por conta da incompreensão da ferramenta. Pra tanto, Maria Cecilia Oliveira Gomes mapeou

[2] ZANATTA, Rafael A.F. *"PROTEÇÃO DE DADOS PESSOAIS COMO REGULAÇÃO DE RISCO: uma nova moldura teórica?"* (2017). Artigos Selecionados REDE 2017. I Encontro da Rede de Pesquisa em Governança da Internet. p. 176.

[3] GOMES**,** Maria Cecília Oliveira. *Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD* (2019), Revista da AASP, n. 144. p. 07.

[4] Kloza, Dariusz & Dijk, Niels & Gellert, Raphaël & Böröcz, István & Tanas, Alessia & Mantovani, Eugenio & Quinn, Paul. (2017). *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals***.** p. 01.

os principais desafios para a regulação do RIPD brasileiro, sugerindo cinco eixos de análise: (i) identificar o que é a ferramenta, as reais funções do relatório e seu papel dentro da LGPD; (ii) a noção de risco e a sua análise e documentação; (iii) as hipóteses de obrigatoriedade de elaboração; (iv) a metodologia adequada para elaboração do relatório; e (v) o estabelecimento de parâmetros para demonstrar a prestação de contas à ANPD, bem como sua eventual publicização.[5]

Tecidas estas breves considerações, o presente artigo científico visa contribuir com o debate nacional acerca do tema, e para isso, buscar-se compreender o que é o relatório, suas reais funções e finalidades, a partir do pano de fundo teórico da abordagens *rights-based* e *risk-based*, traçando um histórico dos predecessores desta ferramenta, começando com as *impact assessments*, com o *Privacy Impact Assessment* nos moldes dados pelo *Information Comissioneer's Office (ICO)* e com o *Data Protection Impact Assessment (DPIA)* do *General Data Protecion Regulation (GDPR)* da União Europeia, que culminou no nosso Relatório de Impacto à Proteção de Dados (RIPD).

2 A VIRADA REGULATÓRIA

O pano de fundo teórico em que esses tipos de ferramentas se originaram é o debate acerca das abordagens regulatórias baseadas nos direitos fundamentais (*rights-based approach)* e no risco (risk-based approach). A compreensão disso é fundamental para a compreensão da ferramenta.

Autores como Rafael F. A. Zanatta entendem que não há uma dicotomia propriamente dita entre as abordagens *rights-based* e *risk-based* nessa "guinada teórica[6]", mas sim uma "fricção" entre elas, em que a sistemática de avaliação de riscos é incorporada no modelo teórico da proteção dos direitos fundamentais. Todavia, a risquificação da proteção jurídica aos

[5] GOMES, Maria Cecília Oliveira. *Desafios da Regulamentação do Relatório de Impacto (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. p. 04.

[6] Zanatta entende por "guinada teórica" justamente esse processo de incorporação do modelo baseado em risco ao modelo regulatório dos direitos fundamentais no debate da proteção de dados pessoais.

direitos fundamentais pode ser fragilizada consideravelmente quando a abordagem baseada em riscos é incorretamente incorporada ou aplicada.[7]

O debate da fricção entre os modelos teóricos é rico e atual. A título de exemplo, a ONG *Access Now*, cujo foco é a defesa dos direitos civis digitais, em resposta à consulta pública da proposta de regulamentação em aplicações que usam inteligência artificial do parlamento europeu, criticou fortemente a abordagem baseada em riscos quando aplicada a regulação de aplicações que utilizam de Inteligência Artificial.

As críticas principais foram que o *GDPR* não é uma regulamentação baseada em risco, e que os pontos do regulamento geral europeu, em que predominam a análise de risco, revelaram-se problemáticos por diversos fatores[8], destacando-se o caráter altamente imprevisível que sistemas de inteligência artificial podem tomar se pertencentes a uma "zona cinzenta" nas avaliações de risco. Então, um sistema, cujas consequências aos titulares são altamente imprevisíveis, pode ser classificado pela autoridade de *enforcement* ou pelo controlador como de baixo-risco, e por consequência, são desnecessárias medidas adicionais de mitigação desses riscos, o que pode gerar consequências catastróficas ou uma violação direta aos direitos e liberdades fundamentais dos titulares.

Outro ponto interessante destacado foi o de que uma iniciativa que utilize de I.A. pode ser frontalmente contrária aos direitos do titular e à legislação, e mesmo assim, ser implementada e utilizada, confundindo o que é violação direta (ou *non-compliance)* com risco, relegando a sua análise para uma fase posterior da avaliação de impacto, o que medida nenhuma de mitigação pode corrigir ou remediar, situação esta que enfraquece os mecanismos de prevenção e proteção aos titulares como um todo. [9]

Esse tipo de confusão ocorreu no cenário regulatório europeu, cujos agentes, como os órgãos de governo e a sociedade civil, possuíam considerável maturidade atinente ao tema de proteção de dados, levando em consideração a Diretiva 95/46/EC, vigente desde 1998, sem

[7] ZANATTA, Rafael A.F. *PROTEÇÃO DE DADOS PESSOAIS COMO REGULAÇÃO DE RISCO: uma nova moldura teórica?* (2017). Artigos Selecionados REDE 2017. I Encontro da Rede de Pesquisa em Governança da Internet. p. 176.

[8] As avaliações de risco no GDPR ocorrem tipicamente na elaboração do DPIA e quando há incidentes de segurança.

[9] Access Now. *The EU should regulate AI on the basis of rights, not risks***.** 17 de fevereiro de 2021. Disponível em: https://www.accessnow.org/eu-regulation-ai-risk-based-approach/.

contar com as diversas leis nacionais dos estados-membros, cujas origens datam da década de 1970.

A confusão consistia no crescente entendimento equivocado de que as abordagens baseadas em risco seriam uma substituição ao modelo baseado nos direitos de proteção de dados pessoais e de seus princípios.

Para tanto, a *Working Party 29* (WP29), em 30 de maio de 2014, emitiu um parecer técnico sobre a função das abordagens em risco no *framework* regulatório de proteção de dados pessoais, visando esclarecer tal problemática e as questões levantadas pelos vigorosos debates da época.

Nessa esteira, o ponto fulcral das ferramentas *risk-based* é o de que estas têm como função uma abordagem *escalável e proporcional ao compliance*, isto é, para o controlador, cujas atividades de processamento de dados são de baixo risco, não há necessidade de fazer tanto para se adequar[10] às suas obrigações legais quanto um controlador cujo processamento tenha alto risco.[11]

As obrigações de adequação à lei dos controladores e operadores permanecem as mesmas, principalmente no tocante aos direitos do titular (como os direitos de acesso, portabilidade dos dados, etc.) e aos princípios do GDPR, independente do risco do processamento. O que pode sofrer alterações é justamente a obrigação de demonstração (incluídas as de documentação e de medidas adicionais de mitigação de risco) desse *compliance*.

Quanto aos princípios aplicáveis aos controladores, permanecem os mesmos, independentemente dos riscos do processamento. Todavia, a WP29 faz uma ressalva:

> "Os princípios fundamentais aplicáveis aos controladores (ou seja, legitimidade, minimização dos dados, limitação da finalidade, transparência, integridade dos dados, precisão dos dados) devem permanecer os mesmos, independentemente do processamento e dos riscos para os titulares dos dados. No entanto, a devida consideração à natureza e ao escopo de tal processamento sempre foram parte integrante da aplicação desses princípios, de modo que eles são inerentemente escaláveis"[12]

[10] E por consequência lógica, comprovar sua adequação, em atenção ao princípio do *accountability.*

11 WP29, *"Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks"* (2014). p. 2.

[12] "Fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable". Ibidem. p.3.

A WP29 traz a presença dos vocábulos "adequado", "apropriado", "razoável" e "necessário" dos artigos 6º e 7º, da Diretiva 95/46/EC. Por exemplo, o juízo de adequação de necessidade ou de razoabilidade do tratamento de dados, com as finalidades almejadas, é inerente a tais princípios, e nenhum controlador pode furtar-se de observá-los. Aqui, o elemento "risco" não é determinante para a aplicação correta dos princípios ao caso concreto. Todavia:

> "as obrigações dos controladores por meio de ferramentas e medidas de responsabilidade (por exemplo, avaliação de impacto, proteção de dados desde o projeto, notificação de violação de dados, medidas de segurança, certificações) podem e devem ser variadas de acordo com o tipo de processamento e os riscos de privacidade para os titulares dos dados. O que pode variar, entretanto, é o nível de obrigações de prestação de contas, que dependerá do risco da atividade." (tradução livre)[13]

Tanto na sistemática da Diretiva 95/46/EC, do *GDPR* e da LGPD, a obrigação de documentar as atividades de processamento e de implementar medidas de segurança mínimas para resguardar os direitos do titular são gerais e indistintas,[14] independente do alto ou baixo risco da operação, mas há obrigações específicas que são desencadeadas em momentos específicos. A régua escolhida pela Diretiva e pelo *GDPR*, que determina essa escalabilidade de obrigações para os agentes de tratamento, é o fator "alto risco ao titular".

O que pode variar é a *forma* com que estes riscos são identificados, avaliados, mitigados e documentados, e a *forma* escolhida pela lei é, para tanto, uma avaliação de impacto, gênero no qual o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), o DPIA e o PIA são espécies.

Então, sob a égide da proteção de dados pessoais dos indivíduos e de seus direitos e liberdades fundamentais, não basta somente uma dicotomia purista de modelos regulatórios. Tampouco basta a pura e simples incorporação de elementos de risco nas legislações, principalmente em proteção de dados. É preciso delimitar bem as bases teóricas e premissas nas quais estas avaliações de riscos são fundadas, não somente para fins de esclarecimento e correta aplicação de tais ferramentas pelos controladores, mas para a eficácia máxima de todo o sistema.

---

[13] Ibidem. p.3.

[14] Dialogando com a LGPD, isso pode ser extraído dos princípios da segurança, da prevenção e da responsabilização e prestação de contas (art. 6º, incisos VII, VIII e X) e do art. 46, caput, da lei, sem prejuízo de o.tros: "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

3 BREVE HISTÓRICO DAS FERRAMENTAS

a) As *Impact Assessments* (Avaliações de Impacto)

As *Impact Assessments* surgiram nessa virada regulatória mundial, que saiu da órbita predominantemente fiscalizatória e repressiva para uma concentração de esforços por parte dos órgãos competentes e dos agentes econômicos em evitar ao máximo que ocorra o evento danoso, seja ambiental, nuclear, biotecnológico ou em proteção de dados.

As *Impact Assessments (IA)* podem ser definidas como:

> "um processo estruturado para considerar as implicações, para as pessoas e seu ambiente, das ações propostas, enquanto ainda há uma oportunidade de modificá-las (ou mesmo, se for o caso, abandoná-las). É aplicado em todos os níveis de tomada de decisão, desde políticas a projetos específicos"[15].

Roger Clarke as sistematizou e classificou de acordo com o enfoque que dão[16]:

> **Foco em tecnologia**
>
> ● *Technology* (Impact) *Assessment* (TA) – Avaliação de Impacto Tecnológico. Foca em uma tecnologia em geral. Ex. Identificação por radiofrequência (RFID), inteligência artificial, *machine learning*, medidores *smart*, drones, blockchain, etc.
>
> **Foco em projetos**
>
> ● *Technology Application Impact* Assessment – Avaliação de Impacto à Aplicação Tecnológica.
> Foca no uso específico de uma tecnologia ou mais, combinada com processo (ou método) de negócio e/ou disposições regulatórias. Ex. Identificação RFID em roupas, Inteligência Artificial em reconhecimento de linguagens, medidores *smart* em eletrodomésticos, drones para uso policial, etc.
> ● *Security Impact Assessment* / *Threat Risk Assessment* (TRA) – Avaliação de Impacto à Segurança ou Avaliação de Riscos de Ameaças.
> Foca nos impactos ou nos riscos em segurança de ativos.
>
> **Foco em impacto social**
>
> ● *Social Impact Assessment* – Avaliação de Impacto Social
> Foca nos impactos a valores sociais
> ○ *Rights Impact Assessment* – Avaliação de Impacto à Direitos Fundamentais
> Foca nos impactos aos direitos humanos, fundamentais e liberdades civis.
> ○ *Ethical Impact Assessment* – Avaliação de Impacto Ético
> Foca nos problemas ou dilemas éticos surgidos com o desenvolvimento de novas tecnologias.
> ● *Surveillance Impact Assessment* – Avaliação de Impacto à Vigilância[17]
> Foca nos impactos das tecnologias de vigilância nas múltiplas dimensões da privacidade.

[15] "Impact assessment (IA) is a structured process for considering the implications, for people and their environment, of proposed actions while there is still an opportunity to modify (or even, if appropriate, abandon) the proposals. It is applied at all levels of decision-making, from policies to specific projects". Disponível em: https://www.iaia.org/wiki-details.php?ID=4.

[16] CLARKE, Roger. *Approaches to Impact Assessment (2014). Exhibit 1: Assessment Categories***.** According to Focus. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html#AF.

[17] Interessante ressaltar que esta avaliação está prevista no anteprojeto da Lei de Proteção de Dados para segurança pública e persecução penal, batizado de LGPD Penal.

> ● *Privacy Impact Assessment* (PIA) – Avaliação de Impacto à Privacidade
> Foca nos impactos em todas as dimensões da privacidade.
> ● *Data Privacy Impact Assessment* (DPIA - Tipo 1) – Avaliação de Impacto à Privacidade Informacional
> Foca nos impactos na dimensão de privacidade informacional (*data privacy*/*information privacy)*
>
> **Foco em Compliance**
>
> ● *Regulatory Compliance*
> Foca na adequação/conformidade de uma proposta ou prática com todas as normas relevantes:
> ○ Instrumentos auto-regulatórios organizacionais. Ex. Códigos de Ética.
> ○ Instrumentos auto-regulatórios da indústria. Ex. Códigos de prática da indústria, padrões internacionais de processos e técnicas.
> ○ Instrumentos co-regulatórios. Ex. Os códigos de boas práticas previstos no art. 50 da LGPD; e
> ○ Instrumentos regulatórios formais.[18]
> ● *Legal Compliance*
> Foca na adequação de uma proposta ou prática perante todas as leis relevantes:
> ○ *Privacy Law Compliance*, i.e. adequação com todas as normas jurídicas e jurisprudência dominante que envolvam o direito à privacidade.
> ○ *Data Privacy Law Compliance*, i.e. adequação com todas as normas jurídicas e jurisprudência dominante que regulem a dimensão de *data privacy*.
> ● Statutory Compliance
> Foca na adequação de uma proposta ou prática com uma parte específica da legislação:
> ○ *Data Protection Impact Assessment* (DPIA - Type 2)
> Foca na adequação de uma proposta ou prática com o *GDPR* ou o seu equivalente em cada estado membro da UE.

O traço distintivo das *impact assessments* como gênero é a deflagração da ferramenta quando o projeto pode ser modificado substancialmente, apoiando a tomada de decisão dos envolvidos. Já como espécies, as avaliações se diferenciam de acordo com o enfoque ou escopo. Todavia, para o presente artigo, serão analisadas apenas três espécies das avaliações de impacto: *Privacy Impact Assessment (PIA), Data Privacy Impact Assessment (DPIA – Tipo 1), e Data Protection Impact Assessment (DPIA – Tipo 2).*

Como se vê, o foco do PIA é a privacidade do indivíduo, considerada em todas as suas dimensões sociais possíveis, questão essa que não depende *a priori* de proteção normativa; o *Data Privacy Impact Assessment* (DPIA – tipo 1) considera a privacidade informacional, escopo reduzido ao PIA; já o *Data Protection Impact Assessment (DPIA – tipo 2)*, o instrumento previsto no *GDPR* é classificado como uma avaliação com foco na adequação regulatória

[18] Entendo que esta subclassificação específica não se aplica ao direito brasileiro por se tratar da tradição da *civil law* e não da *common law*, razão pela qual os termos *regulatory compliance*, *legal compliance* e *statutory compliance* não serão traduzidos.

de apenas um diploma legal em específico, ou seja, considera os pontos da privacidade informacional que o *GDPR* regulamenta.

A diferenciação do enfoque de avaliação da ferramenta pode parecer apenas acadêmica, mas é crucial para definir os limites da obrigação do controlador, e, portanto, o que pode e o que não pode ser exigido pela autoridade nacional competente.

b) Os precursores do *Privacy Impact Assessment* (PIA) e a sua relação com a Diretiva 95/46/EC

O PIA começou a ser amplamente utilizado por volta da década de noventa[19] em várias jurisdições do globo, mas seu surgimento data suas raízes por volta de 1970.

Os seus precursores diretos foram a ideia de *technology assessment*, utilizada pelo *Office of Technology Assessment (OTA)*, órgão auxiliar do Congresso norte-americano, desde a sua criação (1972) até seu desmantelamento (1995). Apesar de sua extinção nos EUA, este exemplo foi seguido pela Europa, que criou a *European Parliamentary Technology Assessment (EPTA)*, criado em 1990, que permanece na ativa até os dias atuais.

O objetivo desses órgãos, por consequência do relatório elaborado por eles, é avaliar as consequências sociais do uso de certas tecnologias e ciências, apoiando a decisão dos parlamentares.[20] Outros precursores, talvez os mais conhecidos, foram os *Environmental Impact Statements (EIS)* e *Environmental Impact Assessment (EIA)*, sendo este último focado em avaliar as consequências de um projeto da perspectiva ambiental (CLARKE, 2009). Na Europa, já no campo das primeiras leis de proteção de dados do continente, deve-se notar como precursores do PIA os *pre-decisional assessments*, algo como *compliance checking* das leis, e a sistemática de checagem prévia da Diretiva 95/46/CE.[21]

A Diretiva foi a primeira norma geral da União Europeia que regulava a Proteção de Dados Pessoais do bloco, e visava precipuamente favorecer e proteger o livre fluxo de dados dentro da União, os direitos e as liberdades fundamentais dos cidadãos europeus, notadamente o direito à vida privada, considerando as divergências normativas constantes entre legislações

[19] CLARKE, Roger. *An evaluation of privacy impact Assessment guidance documents* (2011), International Data Privacy Law, 2011, Vol. 1, No. 2, p. 111.
[20] Disponível em: https://eptanetwork.org/about/about-epta.
[21] CLARKE, Roger. *Privacy Impact Assessment: Its Origins and Development*, Roger Clarke, Computer Law & Security Review 25, 2 (2009), pgs. 123-135.

nacionais de proteção de dados dos estados membros, e a positivação dos direitos à privacidade e autodeterminação informativa na Carta dos Direitos da UE.

Nos artigos 18 a 20 da Diretiva, o diploma inaugurou a sistemática de notificação e checagem prévia às respectivas Autoridades Nacionais de Proteção de Dados de cada estado membro. Nessa sistemática, a regra geral era que o controlador deveria notificar a autoridade nacional antes de realizar qualquer tratamento de dados total ou parcialmente automatizada, ou o conjunto destas operações, realizados para uma única finalidade ou finalidades semelhantes.

Esta notificação deveria conter, no mínimo: o nome e o endereço do responsável pelo tratamento e, eventualmente, do seu representante; as finalidades do tratamento; a descrição das categorias de pessoas em causa e dos dados ou categorias de dados que lhes respeitem; os destinatários ou categorias de destinatários a quem os dados poderão ser comunicados; as transferências de dados previstas para países terceiros; a descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação do artigo 17[22].

Todavia, os estados membros poderiam dispensar essa obrigação de notificação ou estabelecer uma notificação simplificada, exceções estas relacionadas com atividades de processamento de baixo risco e com a presença do encarregado, nas seguintes hipóteses:

> "2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
> - where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or:
> - where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
> - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive.
> - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

[22] Este artigo estabelecia obrigações operacionais mínimas ao controlador para tratamento de dados realizado, sendo a principal delas o dever de pôr em prática medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, principalmente quando os dados tratados forem transmitidos via rede, e contra qualquer outra forma de tratamento ilícito.

> thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations."[23]

Ao receber a notificação, ou quando a autoridade fosse consultada pelo encarregado de proteção de dados do controlador, ao verificar que a atividade ali descrita apresentava "riscos específicos" aos direitos e liberdades dos indivíduos, procede-se a checagem prévia, analisando tal atividade detalhadamente e autorizando ou não o seu prosseguimento.

Contudo, a sistemática de notificação geral e checagem prévia *(prior checking)* era ineficaz ao objetivo último da Diretiva, o que culminou no seu abandono, com a promulgação do *General Data Protection Regulation* (GDPR), o que será explorado futuramente.

c) O *Privacy Impact Assessment* no Reino Unido

Ainda durante a vigência da Diretiva, o Reino Unido, por meio do *Information Commissioner 's Office* (ICO), sua autoridade de proteção de dados, foi o primeiro país do continente europeu a desenvolver, instrumentalizar e publicar uma metodologia de avaliação de riscos ao direito à privacidade.[24] O *Privacy Impact Assessment Handbook* foi publicado em forma de manual em novembro de 2007 e revisto em julho de 2009.[25]

O ICO concentra as competências regulatórias de agência independente, órgão consultivo e administrativo-sancionador para todo o ecossistema britânico de privacidade e proteção de dados pessoais, unificando assim as políticas, ações e interpretações administrativas que tratam do tema, tanto no setor público como no privado. Hoje, a agência cobre a aplicação dos seguintes diplomas legais: *GDPR, Data Protection Act, Freedom of Information Act, Privacy*

[23] "Artigo 28. 2. Os Estados-membros apenas poderão estabelecer a simplificação ou a isenção da notificação nos seguintes casos e condições:
— se, para as categorias de tratamentos que, atendendo aos dados a tratar, não são susceptíveis de prejudicar os direitos e liberdades das pessoas em causa, especificarem as finalidades do tratamento, os dados ou categorias de dados a tratar, a categoria ou categorias de pessoas em causa, os destinatários ou categorias de destinatários a quem serão comunicados os dados e o período de conservação dos dados;
— se o responsável pelo tratamento nomear, nos termos do direito nacional a que está sujeito, um encarregado da proteção dos dados pessoais, responsável nomeadamente por:
— garantir, de modo independente, a aplicação, a nível interno, das disposições nacionais tomadas nos termos da presente diretiva.
— manter um registo dos tratamentos efetuados pelo responsável do tratamento, contendo as informações referidas no nº 2 do artigo 21".
assegurando assim que os tratamentos não são susceptíveis de prejudicar os direitos e liberdades das pessoas em causa". Tradução oficial em português europeu, com singelas modificações. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[24] Trilateral Research & Consulting. *Privacy Impact Assesment and Risk Management (2013),* p. 06.

[25] Disponível em:
https://webarchive.nationalarchives.gov.uk/20100402122103/http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/0-advice.html.

and Electronic Communications Regulations, Environmental Information Regulations, INSPIRE Regulations, eIDAS Regulation, Re-use of Public Sector Information Regulations, NIS Regulations, Investigatory Powers Act.[26]

Posteriormente à popularização do PIA, o *Cabinet Office*, órgão auxiliar direto do Primeiro-Ministro, reconheceu a eficácia do PIA e estabeleceu a sua obrigatoriedade[27], a partir de julho de 2008, na administração direta e indireta, em caso de novos projetos ou programas que envolvessem quantidades significativas de dados pessoais, como medida mandatória mínima de segurança da informação[28].

Entre as várias definições possíveis para o PIA, adotamos a que seu mentor intelectual principal, Roger Clarke, que comandou a feitura do *Handbook* britânico, entende como a que abarca todos os seus pontos-chave:

> "Privacy impact assessment (PIA) is a systematic process that identifies and evaluates, from the perspectives of all stakeholders, the potential effects on privacy of a project, initiative or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts."[29]

Há ainda a definição de David Wright e Paul De Hert[30]:

> "a methodology for assessing the impacts on privacy of a Project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts."31

Destas definições, podemos identificar os elementos principais do PIA: ser um *processo* (ou procedimento), não apenas o seu resultado, o relatório; levar em consideração os principais tomadores de decisão (*stakeholders*), ou pessoas atingidas, principalmente, o titular dos dados tratados; identificar e avaliar os efeitos da atividade, sejam positivos ou negativos, co-

[26] As competências regulatórias da agência de fiscalizadora podem ter certa influência, ou até mesmo ser determinante, na amplitude do escopo da avaliação, ora mais amplo, abarcando diversos diplomas legais correlatos, ora mais restrito.
[27] David Tancock, Siani Pearson, Andrew Charlesworth. *The Emergence of Privacy Impact Assessments* (2010). p. 19.
[28] Cabinet Office, Cross Government Actions: *Mandatory Minimum Measures* (2008). Seção I, 4.4.
[29] "A Avaliação de Impacto à Privacidade (PIA) é um processo sistemático que identifica e avalia, a partir da perspectiva de todas as partes interessadas, os efeitos potenciais sobre a privacidade de um projeto, iniciativa, sistema ou esquema proposto, e inclui uma busca por maneiras de evitar ou mitigar impactos negativos sobre a privacidade." tradução livre.
[30] Citado por CABRAL, Filipe F. *O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais – Lei nº 13.709/18.* (2019) Tese (Mestrado em Direito) – Faculdade de Direito. Universidade Estadual do Rio de Janeiro. Rio de Janeiro. p. 88
[31] "Uma metodologia para avaliar os impactos na privacidade de um projeto, política, programa, serviço, produto ou outra iniciativa que envolva o processamento de informações pessoais e, em consulta com as partes interessadas, tomar as ações corretivas necessárias para evitar ou minimizar impactos" – tradução livre.

mo riscos; ser o objeto deste processo de avaliação, ou seja, o direito à privacidade do indivíduo; e determinar esforço do controlador em evitar ou mitigar os impactos negativos no direito à privacidade dos titulares.

Roger Clarke sintetiza os pontos-chave mais importantes do PIA, que os diferenciam de outras atividades da organização: (i) o PIA é realizado em um projeto ou iniciativa específico, o que o diferencia de um programa de compliance geral; (ii) o PIA é antecipatório por natureza, conduzido antes ou durante o desenvolvimento de um projeto, ao invés de em retrospecto (diferente de uma auditoria de proteção de dados e um *compliance check*); (iii) o escopo do PIA é amplo em relação às dimensões da privacidade (*privacy of the person, privacy of personal behaviour and privacy of personal communications*, bem como *privacy of personal data),* possuindo escopo bem mais amplo quando comparado com um DPIA; o PIA tem um escopo amplo em relação às expectativas e perspectivas dos envolvidos que refletem e são incorporadas no projeto, levando em consideração os interesses não só da organização (internos) ou de patrocinadores estratégicos, acionistas, etc., mas também dos segmentos populacionais que serão afetados pelo projeto; (v) o PIA tem amplo escopo no que diz respeito às expectativas com as quais os impactos à privacidade são comparados, incluindo aí as aspirações, necessidades e sentimentos das pessoas e considerações de ordem pública, como o impacto e consequências de um tratamento específico para a sociedade, para a segurança nacional, etc., bem como questões de adequação à(s) lei(s) vigente(s) (o que o diferencia de um *compliance check* ou *assessment (*avaliação de conformidade), seja em adequação às leis de privacidade, em geral, ou a estatutos regulatórios específicos, como leis de proteção de dados (que possuem o foco em privacidade informacional (*data privacy)*; (vi) o PIA é orientado na identificação dos problemas e das soluções, ajustando o projeto, em aplicação do *privacy by design*; (vii) a ferramenta dá ênfase no processo de avaliação, incluindo troca de informações entre setores da organização, *stakeholders* e titulares, aprendizagem organizacional e adaptação do projeto; (viii) o PIA exige engajamento intelectual por parte do alto escalão da organização (CEO's, executivos e gerentes seniores, etc.) e não apenas que ele seja elaborado como mera lista de verificação assinalada por funcionários juniores[32].

[32] CLARKE, Roger. *The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR.* For a Panel at CPDP, Brussels, 27 January 2017. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html, págs. 02-03.

O *Privacy Impact Assessment Handbook* nos traz três ferramentas distintas para a organização implementar. São elas: o *PIA*, a checagem de adequação (*compliance checking*[33]) e a auditoria, cada qual com uma função específica. Inicialmente, o *Handbook* parte para a diferenciação entre elas, levando em conta, principalmente, o grau de maturidade e a implementação do projeto ou sistema, visando sua implementação na rotina da organização, e a factibilidade das recomendações contidas no guia, para que não se tornem penduricalhos burocráticos e ineficazes.

O guia recomenda que *compliance checks* e *data protection audits* sejam utilizados para projetos em fase de implementação ou que já estão em curso há algum tempo, e que o PIA seja utilizado em um estágio em que as recomendações por ele apontadas possam realmente influenciar no desenvolvimento do projeto e serem efetivamente implementadas:

> "The nature of the PIA process means that it is best to complete it at a stage when it can genuinely affect the development of a project. Carrying out a PIA on a project that is up and running runs the risk of raising unrealistic expectations among stakeholders during consultation. For this reason, unless there is a genuine opportunity to alter the design and implementation of a project, the ICO recommends that projects which are already up and running are not submitted to a PIA process, but to either a compliance check or a data protection audit, whichever is more appropriate."[34]

A razão disso é que o esforço da organização e os custos para alterar projetos já em curso são muito maiores que as modificações pontuais na fase de *design* e implementação deles. Além disso, auditorias ou *checklists* de *compliance* pressupõem a existência de leis, regulamentos ou outros instrumentos normativos aos quais o projeto precisa ser adequado. Ou há adequação à lei ou não há. Nesse sentido, o escopo de aplicação do PIA é bem mais amplo que o *compliance check*, porquanto avaliar o impacto de um projeto na perspectiva do direito à privacidade não depende necessariamente das leis vigentes, por ser um aspecto antes social do que juridicamente considerado como elemento normativo.

---

[33] O *compliance checking* e a *data protection audit* não são definidos expressamente pelo Handbook. Estes instrumentos são apenas diferenciados por suas vantagens de acordo com o momento adequado de sua implementação ou deflagração. Todavia, podemos extrair que ambos são instrumentos cuja atividade predominante é a de avaliar um projeto já implementado sob a ótica de sua legalidade ou não, indicando os problemas e propondo eventuais mudanças. Não há menção direta, no guia, dos *compliance risks*, ou os riscos de compliance, que é a avaliação de riscos que a organização realiza.

[34] "A natureza do processo do PIA significa que é melhor concluí-lo em um estágio em que possa afetar genuinamente o desenvolvimento de um projeto. Realizar um PIA em um projeto que está funcionando corre o risco de gerar expectativas irrealistas entre as partes interessadas durante a consulta. Por esse motivo, a menos que haja uma oportunidade genuína de alterar o desenho e a implementação de um projeto, a ICO recomenda que os projetos já em funcionamento não sejam submetidos a um processo de PIA, mas a uma verificação de conformidade ou a dados auditoria de proteção, o que for mais apropriado." – tradução livre. ICO. *Privacy Impact Assessment Handbook* – Version 2.0. p. 03.

O guia recomenda que os *compliance checks* sejam feitos no começo de um projeto, embora só possam ser completados quando o projeto atingir uma forma mais concreta e detalhada[35]. O objeto do *compliance*, por sua vez, não considera apenas um diploma legal, mas todas as normas jurídicas que protejam direta ou indiretamente a privacidade do indivíduo[36]. Todavia, o guia não sugere ou aponta que o *compliance check* seja incompatível ou independente do PIA, permitindo a sua incorporação.

d) O *enfoque* do *Privacy Impact Assessment*: as dimensões da privacidade

O PIA deve considerar o projeto ou tratamento de dados (objeto), contrastando-o com o direito de privacidade do titular, em caráter amplo, com todas as suas dimensões (enfoque de análise), como recomenda o *Handbook*. Para o manual, o direito à privacidade está relacionado à integridade do indivíduo, com diferentes aspectos das suas necessidades sociais. Esses aspectos não são definições estritas que esgotam o debate sobre a problemática.

---

[35] *"Compliance checking should be started at an early stage of the project to address issues such as the legality of any proposed course of action, but this work will normally only be completed later, once the design of the project has reached a more detailed stage." – "A verificação de conformidade deve ser iniciada no estágio inicial do projeto para abordar questões como a legalidade de qualquer curso de ação proposto, mas este trabalho normalmente só será concluído mais tarde, uma vez que o design do projeto tenha alcançado um estágio mais detalhado." (tradução livre). ICO. Privacy Impact Assessment Handbook – Version 2.0. p. 4.*

[36] *"While compliance checking as part of a privacy impact assessment (PIA) will focus on laws which affect privacy, organisations will have to consider broader legal compliance as well. Public sector organisations will have to consider the extent of their powers, any obligations they have in relation to the personal information they collect and any prohibitions on the use of that information. Private sector organisations will have to consider industry standards and law.*
Further documents may be relevant, such as codes of conduct and privacy policy statements, particularly where the organisation has provided some form of undertaking to comply with them. This might arise from membership of an association that issues the code, or the terms of a document that the organisation itself has produced. There are also matters of public policy that may not be formally law, but that are generally respected." – "Embora a verificação de conformidade como parte de uma avaliação de impacto de privacidade (PIA) se concentre nas leis que afetam a privacidade, as organizações também terão que considerar uma conformidade legal mais ampla. As organizações do setor público deverão considerar a extensão de seus poderes, quaisquer obrigações que tenham em relação às informações pessoais que coletam e quaisquer proibições de uso dessas informações. As organizações do setor privado terão que considerar as normas e leis do setor. Outros documentos podem ser relevantes, como códigos de conduta e declarações de política de privacidade, especialmente quando a organização forneceu alguma forma de compromisso para cumpri-los. Isso pode surgir da inscrição em uma associação que emita um código de conduta, ou dos termos de um documento que a própria organização produziu. Existem também questões de ordem pública que podem não ser formalmente lei, mas que são geralmente respeitadas." (tradução livre) Ibidem. p. 47.

O manual nos traz quatro aspectos principais do direito[37]: *the privacy of personal information, the privacy of the person, the privacy of personal behavior and the privacy of personal communications.*[38]

A *privacy of personal information*, também referida como autodeterminação informativa, está relacionada à resistência das pessoas em reconhecer que os dados a ela relacionados estejam expostos/acessíveis facilmente a outros indivíduos e organizações. Daí surge o direito de exercer um controle efetivo sobre o dado e como ele é usado.[39]

---

[37] Ibidem. p.14.

[38] Mantive a nomenclatura dos direitos no original por entender que sua tradução direta pode gerar confusões. Mesmo com o esforço máximo, acredito que esses termos são intraduzíveis pela perda de significado de sua gênese. Esta nomenclatura reflete diretamente a própria concepção do Direito para os britânicos. Traço esse paralelo com o seguinte trecho de Pontes de Miranda, ao falar sobre as diferentes concepções de liberdade, comparando as da *common law* e a dos franceses da Revolução de 1789, cujo raciocínio, *mutatis mutandis*, pode ser aplicado com ressalvas à problemática da privacidade: *"Na Inglaterra, a palavra "liberdade", em direito, sempre vem acompanhada de adjetivo ou de atributo: liberdade pessoal, liberdade de imprensa, etc.*
Todavia a Constituição dos Estados Unidos, conquanto muito extraísse do direito inglês, foi contemporânea da liberdade abstrata, indefinível, e ampla dos pensadores franceses. Eis aí a razão de lá se encontrar, por vezes, aquêle vocábulo desgarrado e sibilino: liberty. Foi sinal dos tempos.
Em que consiste essa liberdade misteriosa, demagógica, nós o sabemos de Montesquieu, no capítulo III do livro XI de seu Espirit des lois: "à pouvoir faire ce que l'on doit vouloir, et à n'être point contraint de faire ce que l'on doit ne point vouloir". Pura liberdade à Robinson Crusoe.
A liberdade inglêsa não é essa. Distinguem-se qualitativamente. Nessa divergência está concretizada a diferença dos caracteres psicológicos dos dois povos. Uma é integral, dogmática, abstrata; a outra é concreta: divide-se, tem espécies… Ora a liberdade de imprensa, ora a liberdade de consciência, ora a liberdade física.
Tôdas concernem a algum objeto sensível. Não são figuras metafísicas. Não volteiam nos domínios da ideologia. Tôdas pisam em terra firme. Não querem o infinito, como aquela: apenas exprimem o conteúdo de seus limites. Se é a liberdade física, define-se em termos verbais invariáveis e salientes: ir, ficar e vir.
Dir-se-à que a outra, a de Paris, é mais bela, mais sedutora. Não há dúvida. Porém mais mentirosa. Promete castelos a quem morre de fome: dá todos os direitos, mas faz depender da opinião exegética do Procurador da Republica a locomoção de alguém. Em vez de ser valor restrito e utilizável, não suscetível de servir a outros intuitos, serve aos maus contra os bons.
Que fêz ela? Nada. Aguilhoou o indivíduo. Criou o mais desbragado capitalismo e deu-o aos menos dignos ("a todos", diz-se; mas os menos dignos tem melhores armas) o direito de explorar homens livres. - Todos são livres; escravizai-vos, agora, uns aos outros!
Sempre foi traço de caráter dos povos inglêses essa precisão a respeito de direitos, coisa em que não os imitaram os escritores franceses. Sirva de exemplo o próprio Parlamento francês. A concepção dilatou-se, fêz-se abstrata, expansiva: em vez de continuar o centro do poder britânico, com as Declarações de direitos, mais escritas nas cabeças do que nos livros e nos discursos.
Onde muito se fala em liberdade, pouco ela é defendida. Corajosamente, até a morte, a sustentam os que, em vez de Liberdade, falam, prática e sabiamente, de liberdade física (de ir, ficar e vir), de liberdade de pensamento, de liberdade de religião (criação de Rhode Island, nos Estados Unidos da América), de liberdade de imprensa, etc." (PONTES DE MIRANDA, História e Prática do Habeas Corpus. 2ª Ed. (1955), José Konfino, pg. 31/32.).

[39] "Individuals generally do not want data about themselves to be automatically available to other individuals and organisations." – "Os indivíduos geralmente não querem que seus dados sejam disponibilizados automaticamente para outros indivíduos e organizações" (tradução livre) ICO. Privacy Impact Assessment Handbook. p.14.

A *privacy of the person* ou *bodily privacy* está relacionada à integridade corporal do sujeito, associada normalmente às revistas corporais, à imunização compulsória, à transfusão de sangue sem consentimento, à entrega compulsória de amostras de tecido ou fluidos corporais, entre outros.

A *privacy of personal behaviour* relaciona-se à noção de *private space*, ou seja, o monitoramento do que um indivíduo faz. Das facetas que a privacidade pode ter na concepção dos britânicos, não sendo uma lista exaustiva, esta é a que mais se assemelha ao clássico conceito de privacidade estadunidense - *the right to be let alone* - desenvolvido até a proteção autônoma e constitucional do *right of privacy.*

A *privacy of personal communications* está atrelada a ideia de proteção da comunicação entre dois indivíduos, seja por qualquer meio, da observância de terceiros não integrantes da relação. No direito brasileiro, entendemos esse aspecto como o sigilo das comunicações pessoais.

Nestes termos, o direito à privacidade, em todas as suas dimensões, não pode ser abarcado por um diploma legal específico. Mesmo considerando a proteção à privacidade em todo o ordenamento jurídico, isso pode não ser suficiente para satisfazer as expectativas das pessoas e as consequências negativas que advêm de uma prática invasiva à privacidade delas.

Mesmo assim, o projeto deve ser avaliado sob o ângulo das leis aplicáveis, no mínimo. Porém, um bom PIA não deve se limitar às leis vigentes e aplicáveis ao projeto. As necessidades, expectativas e preocupações dos indivíduos, grupos de indivíduos e comunidades, muitas vezes, não estão refletidas diretamente na legislação vigente. Não é incomum encontrar casos de projetos e sistemas que, embora estejam de acordo com as leis aplicáveis, por não se preocuparem de fato, sofrem uma cobertura negativa da mídia, e por reflexo da opinião pública, o que pode minar sua confiança e acabar com a sua descontinuidade.[40]

e) O *Data Protection Impact Assessment* no *GDPR* e o controle prévio

[40] "Organisations that carry out a DPIA may be fully compliant with data protection legislation, but could still intrude dangerously into an individual's privacy. Such a risk is greatly diminished if all types of privacy are considered, as the ICO Handbook rightly argues.". "Organizações que realizam uma DPIA podem estar em total conformidade com a legislação de proteção de dados, mas ainda podem invadir perigosamente a privacidade de um indivíduo. Esse risco diminui muito se todos os tipos de privacidade forem considerados, como o Manual da ICO corretamente argumenta" (tradução livre). *Privacy impact assessment and risk management* (2013). Report for the Information Commissioner's Office prepared by Trilateral Research & Consulting, p. 149.

Como dito, o sistema de notificação geral e checagem prévia da Diretiva foi substituído, optando-se por outras alternativas mais eficazes à proteção de dados pessoais dos indivíduos, exposta no considerado (ou *recital)* 89 do *GDPR*:

> "Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento."[41]

A consulta prévia (*prior consultation*) consiste em notificar a autoridade nacional respectiva apenas quando há "altos riscos" residuais ao tratamento de dados, isto é, após todas as medidas de mitigação identificadas pelo controlador forem implementadas.

Há duas diferenças na sistemática da Diretiva e do atual *GDPR*: (i) os gatilhos que exigem atuação da autoridade nacional são diferentes. Na primeira, realizava-se a checagem prévia, quando identificados altos riscos iniciais no tratamento, (o risco bruto), e na segunda, somente quando há altos riscos residuais; e (ii) no GDPR, a ausência de resposta da autoridade nacional, quando provocada, não implica em autorização da atividade.[42]

Percebe-se, nesta mudança, que há o constante esforço de afunilamento e aperfeiçoamento para que a atuação das autoridades nacionais se dirija quando ela for *realmente necessária*, concentrando os esforços justamente nas situações mais críticas.

O DPIA deverá prosseguir, de forma que todos os riscos aos direitos e liberdades individuais sejam identificados e avaliados. As medidas de mitigação a esses riscos e salvaguardas deverão ser implementadas, e depois de sua implementação pelo controlador, caso estas se mostrem insuficientes e ainda restem riscos residuais altos que não podem ser mitigados, ou em caso de dúvida na mitigação, o controlador deverá proceder com a consulta prévia à autoridade nacional do respectivo estado membro, para que esta analise o DPIA enviado e forneça o auxílio consultivo necessário.

---

[41] GDPR. Considerando 89.

[42] EDPS. *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation* (2019). p. 21.

Há uma relação entre o registro de atividades de processamento (ROPA)[43], entre os DPIA's e a consulta prévia. O registro é para todas as operações; o DPIA é para operações que apresentam altos riscos aos direitos e liberdades fundamentais do titular; e a consulta prévia, para quando há altos riscos residuais[44]. O *GDPR* estabeleceu como ferramenta típica para avaliação dos altos riscos e sua mitigação o DPIA.

O desenvolvimento e a experiência do Reino Unido popularizaram o uso dos PIA's pela Europa, o que culminou no *Data Protection Impact Assessment* (DPIA). A definição do que é a ferramenta se encontra no artigo 35, 1.:

> "Quando um 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."[45]

O *DPIA* é um processo de avaliação que é deflagrado em um momento bem específico: quando, antes de se iniciar uma atividade de tratamento, identificam-se altos riscos aos direitos e liberdades fundamentais do titular.

A realização do relatório pode ser dispensada quando se verificar que: (i) o tratamento não enseje altos riscos; (ii) quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada um DPIA; (iii) quando as operações de tratamento tiverem sido previamente controladas por uma autoridade de controle do GDPR em condições específicas que não se tenham alterado; e (iv) quando uma operação de tratamento for fundada como necessária para o cumprimento de obrigação legal ou regulatória pelo controlador ou necessária para atender ao interesse público (nos termos do artigo 6º, nº 1, alíneas c) ou e) do GDPR e que tal avaliação já tenha sido realizada como parte da adoção desse fundamento jurídico (GDPR, artigo 35.º, n.º 10), salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tra-

[43] GDPR, Artigo 31.
[44] EDPS. *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation*. (2019). p. 20.
[45] GDPR. Art. 35.1, versão em português europeu.

tamento; ou (v) quando o tratamento for listado pela Autoridade Nacional respectiva como opcional ao DPIA. [46]

Portanto, além de um esforço para concentrar a atuação da autoridade nacional de proteção de dados, há um esforço em manter a máxima clareza de quando o DPIA deve ser deflagrado[47], e, ainda, não onerar desnecessariamente os agentes de tratamento, possibilitando o aproveitamento de avaliações semelhantes, sejam feitas por si ou por outrem, com as respectivas medidas de mitigação.

O relatório deverá ser acompanhado e assinado pelo *data protection officer (DPO),* equivalente ao encarregado da LGPD, nos casos em que for designado. No *GDPR*, é obrigatório designá-lo: (i) caso o controlador seja uma autoridade ou órgão público (exceto para o Judiciário atuando em sua competência jurisdicional); (ii) caso as atividades de tratamento realizem monitoramento regular e sistemático em larga escala dos indivíduos; ou (iii) caso as atividades principais de tratamento de dados do controlador consistam em processamento em larga escala de dados sensíveis ou de dados relacionados a condenações e delitos criminais.

Todavia, a escolha e adoção dessa ferramenta não é imune às críticas, tais como: (i) a de ser um fardo desnecessário, uma burocracia desproporcional, o que causa aumento de despesa e atrasa a tomada de decisão por parte dos agentes de tratamento, e por consequência o desenvolvimento do projeto; (ii) a complexidade do processo de avaliação na prática, as dificuldades que acarreta, a ausência de experiência da organização, bem como ausência de orientação por parte das autoridades competentes; (iii) a incerteza do valor do DPIA em relação a outras técnicas de avaliação (como *compliance checks* ou auditorias), bem como sua eficácia para os direitos dos titulares, considerando a ampla discricionariedade concedida sobre "como" e "se" tais avaliações devem ser conduzidas ou não; (iv) quando o DPIA é exigido por lei em certa hipótese, representa apenas instrumento de *compliance* regulatório, de escopo restrito, o que faz projetos e iniciativas consideravelmente invasivos, perigosos ou danosos serem

46 WP29. *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679* – p. 15.

47 O rol exemplificativo de operações que ensejam em alto risco do GDPR é complementado com um guia de critérios da WP29 sobre operações de tratamento a que o controlador deve ficar atento. Além disso, há as *blacklists* emitidas pelas autoridades nacionais, que são inspiradas nos critérios da WP29 e complementam as hipóteses de alto risco do rol legal. Outro ponto que demonstra isso é o histórico dos pareceres da EDPB sobre as *blacklists* de cada autoridade nacional, zelando pela integridade e semelhança do *GDPR* no bloco, e portanto, da clareza dos critérios.

desconsiderados; v) a falta de transparência, tendo em vista a complexidade da análise ou do projeto em si mesmo considerado, e, por conseguinte, de resultados finais e recomendações, o que torna a avaliação opaca ao escrutínio público e aos afetados pela iniciativa; vi) além da opacidade, a consulta pública e dos afetados pelo tratamento, por estarem sujeitos ao juízo de discricionariedade do controlador dos dados, tornam-se mero "faz de conta".[48]

Roger Clarke tece diversas críticas sobre o DPIA, em ocasião do então recém aprovado artigo 35.1 do GDPR: (i) o DPIA não é movido por valores sociais; (ii) será interpretado apenas como uma *Data Protection Law Compliance Assessment (*i.e. uma avaliação de *compliance* com certa lei de proteção de dados); (iii) possui escopo de proteção reduzido quando comparado com avaliações de impacto à privacidade informacional (*data privacy*), e menos ainda quando comparado com o PIA, que encampa todas as dimensões da privacidade. (iv) quanto ao escopo de atuação, aplica-se apenas ao subconjunto de interesses (ou pretensões) relativas à privacidade informacional do titular regulados por uma lei de proteção de dados vigente, escopo de proteção bem reduzido se o objeto de adequação da avaliação fosse o impacto à privacidade informacional, ou mesmo em caso de adequação a todas as leis/regulamentações vigentes acerca de privacidade informacional;[49]

Além disso, Clarke aponta que as organizações já estão sujeitas à obrigação de se adequar a lei em caso de implementação de novas iniciativas e projetos, o que o torna desnecessário, e que as inovações do art. 35 do GDPR em nada avançam em proteção à privacidade, citando um leve progresso em relação às obrigações de descrição sistemática do tratamento e da avaliação da necessidade e proporcionalidade do tratamento (GDPR, Art. 35, 7.). Para elucidar tais críticas, Clarke propõe uma situação hipotética, de modo a convidar o leitor à reflexão:

> "CCTV, body-worn cameras and drone-borne cameras may record data. But they can also stream data to an observer without recording it. And they can also cause people concern just by being there without being switched on - and indeed the mere possibility that they may be around is upsetting to various individuals under various circumstances.
> Where visual surveillance doesn't give rise to any recorded data:
> (a) can a DPIA consider the impact on the privacy of personal behaiour of:

[48] Kloza, Dariusz & Dijk, Niels & Gellert, Raphaël & Böröcz, István & Tanas, Alessia & Mantovani, Eugenio & Quinn, Paul. (2017*). Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals*. p. 03.

[49] CLARKE, Roger. *The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR.* For a Panel at CPDP, Brussels, 27 January 2017. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html. p. 03.

(i) the operation of cameras?
(ii) the existence of cameras?
(iii) the possibility of the existence of cameras?
(b) *must* a DPIA ... (etc.)?"[50]

f) O elemento alto risco

i. Riscos de compliance e riscos ao titular

Como se viu anteriormente, tanto no PIA quanto no DPIA, a ferramenta torna-se obrigatória a partir da identificação do elemento "riscos específicos" ou "altos riscos" – que podem ser entendidos como sinônimos. A obrigatoriedade de elaboração do DPIA é extraída: (i) das listas de operações de alto risco emitidas pela autoridade nacional competente; ou (ii) da avaliação inicial de riscos do tratamento, feita pelo próprio controlador.[51] Em ambas as ocorrências, pode-se ver que a presença do elemento "alto risco" é imprescindível para que a ferramenta se torne obrigatória.

Inicialmente, cabe ressaltar que os riscos em proteção de dados possuem ângulos distintos de análise. Pode-se analisá-los do ponto de vista da organização e do ponto de vista do titular. Os primeiros são os riscos de *compliance*, ou seja, os riscos que a organização corre em não se adequar à legislação, que também podem abarcar danos na sua imagem, em descontentamento social, etc. Os segundos são os riscos aos direitos e às liberdades fundamentais do titular. No DPIA, os riscos devem ser avaliados primariamente do ponto de vista do titular de dados, mas nada impede que o mesmo relatório contenha uma avaliação de riscos de *compliance.*[52]

---

[50] Ibidem. CFTV (circuito fechado de televisão), câmeras corporais e câmeras portadas por drones podem registrar dados. Mas eles também podem transmitir dados para um observador sem gravá-los. E também podem causar preocupação às pessoas apenas por estarem presentes sem estarem ligados - e, de fato, a mera possibilidade de que possam estar por perto é perturbadora para vários indivíduos em várias circunstâncias.
Onde a vigilância visual não dá origem a nenhum dado registrado:
(a) um DPIA pode considerar o impacto sobre a privacidade do comportamento pessoal:
(i) do funcionamento das câmeras?
(ii) da existência de câmeras?
(iii) da possibilidade da existência de câmeras?
(b) * deve * um DPIA fazê-lo?... (etc.)?" (tradução livre).

[51] EDPS. *Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments (*2018). p. 09.

[52] "*In a DPIA, you assess primarily risks to the rights and freedoms of data subjects. At the same time, you should analyse the compliance risks for your organisation. These are related, but not necessarily identical."* – " Em um DPIA, você avalia principalmente os riscos aos direitos e liberdades dos titulares dos dados. Ao mesmo tempo, você deve analisar os riscos de conformidade para sua organização. Eles estão relacionados, mas não necessariamente idênticos." (tradução livre). EDPS. *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation* (2019)**.** p. 08.

Pode-se encontrar uma elucidação de como o risco pode ser materializado para o titular no Considerando 75, do GDPR:

> "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados."[53]

É importante considerar, no DPIA, todo e qualquer risco que possa prejudicar, direta ou indiretamente, a autonomia individual da pessoa em causa, e isso leva em consideração impactos emocionais como o medo, a angústia, a supressão, ou o efeito inibidor que certo tratamento pode gerar nos direitos e nas liberdades fundamentais, como, por exemplo, vigilância, controle e rastreamento contínuo, afetando potencialmente as liberdades de ir e vir, de intimidade, e de liberdade de expressão, além de, principalmente, os aspectos de probabilidade do evento danoso e da severidade do dano.

Outro ponto importante é que o "impacto" avaliado não deve ser somente considerado no eixo da quantidade. Não se pode avaliar o risco unicamente na quantidade de pessoas afetadas pelo processamento. Sem dúvida, este é um fator importante, mas o principal a ser considerado é o eixo qualitativo, que é justamente o impacto nos direitos e nas liberdades não só do titular individualmente considerado, mas da sociedade como um todo.

A avaliação de riscos inerentes ao tratamento não deve se resumir a precauções contra incidentes de segurança. Projetos que envolvam o uso de novas tecnologias, por exemplo, podem causar um dano muito mais acentuado se realizado de uma maneira imprudente, como

[53] Versão em português europeu.

um tratamento discriminatório ilícito, causado por dados enviesados e utilizados para o treinamento do aprendizado de máquina.

A análise do elemento risco, portanto, não está limitada a riscos de *compliance*, de descumprimento da lei, a riscos que atentem contra a dimensão da *data privacy*, do indivíduo, a riscos que atentem contra sua privacidade, considerando todas as dimensões envolvidas. Os riscos devem ser avaliados levando-se em conta os direitos e as liberdades fundamentais. Neste ponto, não há como traçar uma régua limite, e tudo que puder afetar negativamente o titular deve ser considerado para que seja mitigado posteriormente.

ii. A obrigatoriedade do DPIA

O GDPR exigiu a elaboração do relatório, estabelecendo que certos tipos de tratamento, por sua natureza, âmbito, contexto e finalidade, podem implicar em um elevado risco para os direitos e as liberdades das pessoas, e nestes casos o controlador deverá, antes de iniciar o tratamento, proceder com um DPIA[54].

O Regulamento exemplificou algumas operações típicas de ensejar num alto risco, e por conseguinte, sua obrigatoriedade: (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 dados pessoais sensíveis ou equiparados ou relacionados com condenações penais, infrações, medidas de segurança e afins; e (c) controle sistemático de zonas acessíveis ao público em grande escala.[55]

O relatório deve conter, no mínimo: "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 direitos a que se refere o nº 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

[54] GDPR, Art. 35, item 1.
[55] GDPR, Artigo 35, versão em português europeu.

o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa"[56].

Ainda, o Regulamento estabelece competência para cada Autoridade de Nacional de Proteção de Dados de cada Estado Membro estabelecer, baseados nos critérios elaborados pelo *Working Party 29*, expostos a seguir, uma lista de operações de "alto risco", tendo como consequência a necessidade de consulta prévia à autoridade para iniciar o tratamento. Essa formulação legal teve como base os estudos realizados pelo WP29, hoje substituído pelo Comitê Europeu para a Proteção de Dados (EDPB), intitulado *"Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679"*.

O WP29 estabeleceu nove critérios em que a operação de tratamento enseja num alto risco, e pontuou que, na maioria dos casos, se a atividade de tratamento "cair" em pelo menos dois critérios, a feitura do DPIA é recomendada. Os critérios são:

> "1. Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de «aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados» (considerandos 71 e 91 da GDPR).
> 2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar: tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza «efeitos jurídicos relativamente à pessoa singular» ou que «a afetem significativamente de forma similar» (artigo 35.º, n.º 3, alínea (a).
> 3. Controle sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um «controlo sistemático de zonas acessíveis ao público» (artigo 35.º, n.º 3, alínea (c).
> 4. Dados sensíveis ou dados de natureza altamente pessoal: inclui categorias especiais de dados pessoais, tal como definido no artigo 9.º (por exemplo, informações acerca das opiniões políticas dos indivíduos), bem como dados pessoais relacionados com condenações penais e infrações, tal como definido no artigo 10.º.
> 5. Dados tratados em grande escala: o RGPD não define o que constitui grande escala, contudo o considerando 91 fornece alguma orientação. Em qualquer caso, o Grupo de Trabalho do Artigo 29.º recomenda que os seguintes fatores, em especial, sejam considerados quando se determina se o tratamento é ou não efetuado em grande escala:
> a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
> b. o volume de dados e/ou a diversidade de dados diferentes a tratar;
> c. a duração da atividade de tratamento de dados ou a sua pertinência;
> d. a dimensão geográfica da atividade de tratamento.
> 6. Estabelecer correspondências ou combinar conjuntos de dados: por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados.

[56] GDPR, artigo 35, nº 7. versão em português europeu.

> 7. Dados relativos a titulares de dados vulneráveis (considerando 75): o tratamento deste tipo de dados constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos. Os titulares de dados vulneráveis podem incluir crianças, empregados, segmentos mais vulneráveis da população que necessitem de proteção especial (pessoas com doenças mentais, requerentes de asilo, idosos, doentes, etc.) e todos os casos em que possa ser identificado um desequilíbrio na relação entre a posição do titular dos dados e o responsável pelo tratamento.
> 8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, tais como combinar a utilização da impressão digital e do reconhecimento facial para melhorar o controlo do acesso físico, etc. O RGPD deixa claro (artigo 35.º, n.º 1, e considerandos 89 e 91) que a utilização de uma nova tecnologia, definida em «conformidade com o nível de conhecimentos tecnológicos alcançado» (considerando 91), pode desencadear a necessidade de realização de uma AIPD. As consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Uma AIPD ajudará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos. Por exemplo, algumas aplicações da «Internet das Coisas» podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD.
> 9. Quando o próprio tratamento impede os titulares dos dados «de exercer um direito ou de utilizar um serviço ou um contrato» (artigo 22.º e considerando 91). Estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato."[57]

g) O RIPD e o pia na lei geral de proteção de dados pessoais

i. A Avaliação de Impacto à Privacidade

Inicialmente, é possível extrair do texto da LGPD a presença tanto de uma avaliação de impacto à privacidade, especificamente no art. 50, §2º, inciso I, alínea (d)[58], como de um relatório de impacto à proteção de dados pessoais (RIPD), em capítulos e momentos distintos. A avaliação de impacto à privacidade, como regulamentada na LGPD, é substancialmente diferente do RIPD. A primeira ferramenta é medida de boas práticas, enquanto a segunda é

[57] WP29. *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 (2017)*. Versão em português europeu. p. 10-12.

[58]: "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
I - implementar programa de governança em privacidade que, no mínimo:
d) estabeleça políticas e salvaguardas adequadas *com base em processo de avaliação sistemática de impactos e riscos à privacidade"*.

obrigatória assim que preenchidas certas condições, de modo que não elaborar um RIPD, quando necessário, pode ensejar em sanções.

Essa avaliação sistemática de impacto à privacidade representa uma semelhança maior com o *Privacy Impact Assessment*, que possui *enfoque* de avaliação bem mais amplo do que o RIPD, que, seguindo os passos do *GDPR,* é uma ferramenta para demonstrar *compliance*. Por estas razões, discordamos da afirmação de Maria Gomes sobre a menção à avaliação sistemática de impactos e riscos à privacidade na lei:

> "se apresenta como uma fase predecessora da elaboração do relatório, uma vez que é necessário primeiro verificar, através de uma avaliação, conduzida e estruturada mediante uma metodologia, sendo, neste caso, uma metodologia avaliativa de riscos, o impacto de operações de tratamento em liberdades civis e direitos fundamentais do ser humano, aqui compreendido como titular dos dados[59].

A lei brasileira, ainda, estabelece a obrigação do controlador em realizar e documentar avaliações de risco, notadamente em três hipóteses: (i) na elaboração e documentação do Relatório de Impacto à Proteção de Dados Pessoais (RIPD); (ii) para saber se comunicará ou não a ANPD acerca do incidente de segurança[60]; e (iii) na avaliação se o tratamento está em desacordo com a legislação, avaliando *"o resultado e os riscos que razoavelmente dele se esperam"*[61]. Desse modo, a LGPD segue a mesma abordagem do GDPR: uma abordagem regulatória baseada em direitos fundamentais com situações específicas de análise de risco.

ii. O Relatório de Impacto à Proteção de Dados

Quanto ao RIPD, a sua importação em um cenário como o brasileiro e a ótica que lhe tem sido dada revelaram-se problemáticas e desafiadores por diversos fatores. Em seu glossário, a LGPD traz o relatório como *"documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco"*[62]. 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 aná-*

[59] GOMES, Maria Cecília Oliveira. *Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD* (2019), Revista da AASP, n. 144. p. 07.
[60] LGPD, Art. 48. *"O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*". À semelhança do GDPR, este artigo traz a possibilidade de que a ANPD considere a desnecessidade de comunicação de incidentes de segurança que entender como irrelevantes aos titulares, o que implica uma avaliação do risco, mesmo que simplificada.
[61] LGPD, Art. 44, inciso II.
[62] LGPD, Art. 5º, inciso XVII.

lise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."[63]

Na definição dada pela LGPD e no conteúdo mínimo do relatório, analisando apenas a letra fria da lei, podemos perceber que ele se distancia bastante da definição dada pelo GDPR, com os conceitos-chaves de processo, de "alto risco", da avaliação de necessidade do tratamento, entre outros, inicialmente ignorados. A única menção ao "alto risco", o que é elemento central do PIA e do DPIA, se encontra no Art. 55-J, inciso XIII da lei:

> "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".

Na verdade, o "relatório de impacto" como insculpido na lei[64] assemelha-se muito mais à junção do *Record of Processing Activities* (ROPA) com uma espécie de *risk assessment.*

Traçando um paralelo com o cenário europeu, no qual o DPIA sofreu diversas críticas, no Brasil, destacam-se alguns agravantes: a abordagem excessivamente formalista que é possível extrair do texto da lei; uma possível amplitude das suas hipóteses de elaboração sem uma proporcionalidade aparente, despregada das reais funções da ferramenta e a ausência de critérios claros para quando elaborá-lo, o que não passou incólume a críticas. Matheus Sturari, a título de exemplo, explorou tais pontos problemáticos extraídos da lei:

> "Constata-se, por dedução da definição do art. 5º, XVII, que o DPIA será exigido para atividades de tratamento que gerem *riscos às liberdades civis e direitos fundamentais.* Entretanto, são várias as dúvidas que permanecem, por exemplo: (i) toda hipótese de tratamento fundamentado em legítimo interesse deve ser acompanhada de um DPIA?; (ii) quais são os tratamentos que serão considerados como geradores

[63] LGPD, art. 38, parágrafo único.

[64] Na LGPD, no texto da lei somente há obrigação expressa do controlador em manter o registro de atividades de tratamento, sem maiores detalhes, o que está previsto art. 37, caput: *"O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."* Logo em seguida, há uma previsão legal do poder da ANPD em requisitar a elaboração do relatório: *"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"*. Estes dois elementos dão a entender que o registro das operações de tratamento e o relatório de impacto são ferramentas autônomas e independentes, em contraposição com a interpretação literal da definição legal do RIPD (inciso XVII do art. 5º) e de seu conteúdo (parágrafo único do art. 38).

> de riscos a ponto de demandarem um DPIA?; (iii) a despeito de uma lista, quais critérios devem ser considerados para analisar a existência de risco e considerar a necessidade de um DPIA?; (iv) todo e qualquer risco deve ensejar um DPIA ou apenas "alto" risco, como no inciso XIII do art. 55-J?"[65]

Destaca-se, também, a sua crítica:

> "Tais dúvidas parecem surgir em razão de uma preocupação da LGPD sob aspecto formal relacionado ao DPIA, isto é, estabelecendo o que deveria ser considerado em seu instrumento (relatório), mas ausência de tratativa, pela lei, referente ao seu aspecto processual, ou seja, não como um mero documento, mas como um processo de análise que deve ser desencadeado de acordo com critérios claros e, preferencialmente, dotados de certo aspecto objetivo. A LGPD parece focar no resultado de DPIA -- o relatório --, mas pareceu silenciar acerca de todo o processo necessário para se chegar a tal relatório, inclusive o principal -- quando tal processo deve ser desencadeado. Acontece que, a existência de tais dúvidas e de um cenário de incertezas envolvendo o tema, tem gerado um efeito que, a meu ver, pode não ser positivo: a possível banalização do DPIA e consequente excessiva oneração dos agentes de tratamento." (grifos do autor).[66]

Estes fatores não indicam uma interpretação nacional, adaptada ao cenário regulatório brasileiro de proteção de dados, mas uma possível "banalização" da ferramenta, na expressão de Matheus Sturari. Nesse mesmo sentido, segue a crítica de Filipe Fonteles Cabral:

> "há o risco de que o RIPD se torne um instrumento de controle em casos isolados ou, pior, que seja um documento elaborado para fins formais, porém sem guiar uma atividade real de gerenciamento de riscos, o que pode comprometer a eficácia do sistema de proteção aos dados pessoais no Brasil."[67]

Os autores nacionais tendem a ressaltar o caráter procedimental, de *documento-vivo,* do relatório, justamente para reverter as incongruências da lei, que resultaria na ineficácia do relatório e do sistema de proteção de dados como um todo.

Todavia, o problema não termina aí. Na evolução das ferramentas, houve um constante esforço para otimizar a atuação das autoridades de proteção de dados nos casos *realmente necessários* e para não onerar excessivamente o controlador de dados com o processo complexo de análise que é uma avaliação de impacto.

---

[65] STURARI, Matheus. *O DPIA na LGPD: interpretação nacional ou banalização do instrumento***?** Perfil do LinkedIn. Publicado em 29 de outubro de 2020. Disponível em: https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpreta%C3%A7%C3%A3o-nacional-ou-banaliza%C3%A7%C3%A3o-do-matheus/.

[66] Ibidem.

[67] CABRAL, Filipe F. *O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais – Lei nº 13.709/18. (*2019) Tese (Mestrado em Direito) – Faculdade de Direito. Universidade Estadual do Rio de Janeiro. Rio de Janeiro. p. 82.

Ocorre que, a mera possibilidade de o relatório ser requisitado[68] diretamente por uma autoridade, para além do critério de alto risco, vai na contramão do controle prévio do *GDPR*, e até mesmo da checagem prévia da Diretiva.

A presença do encarregado de dados e as suas garantias de independência existem justamente para que este realize a comunicação com a ANPD, e não o inverso. Além disso, um eventual cenário de frequente requisição direta de elaboração do relatório pela ANPD demonstra dois sintomas: o primeiro, os critérios para a sua obrigatoriedade não são claros o suficiente, o que pode ser corrigido via ato normativo da autoridade; o segundo, o fracasso completo do RIPD como ferramenta *ex ante,* visto que se os critérios para a sua obrigatoriedade são obscuros, tampouco impedem a implementação de processamento, prossegue-se com a atividade de alto risco, para elaborar o relatório apenas quando solicitado diretamente. Em suma, uma verdadeira carta-branca para o não cumprimento da obrigação de *compliance*.

A Autoridade Nacional teria que, às cegas, identificar os controladores cujas atividades atraiam a necessidade de *enforcement*, requisitar a elaboração do relatório, dar um prazo específico, receber o relatório, avaliar se ele foi elaborado corretamente, se há altos riscos iniciais, e se há altos riscos residuais, para então conseguir auxiliar o controlador e verificar a conformidade.

Esse tipo de abordagem dissipará o tempo e esforço da recém-criada ANPD para onde ela é realmente necessária. O momento mais adequado para a identificação, pela ANPD, se o controlador cumpriu com as suas obrigações de elaborar o RIPD (avaliar conformidade, identificar riscos e mitigá-los) é em uma notificação de vazamento de dados.

Além de estar sujeito a pura discricionariedade, ou na melhor das hipóteses, de uma discricionariedade vinculada, a requisição pode onerar os controladores que não possuem atividades de alto risco, apenas porque uma autoridade requisitou o relatório, que será feito às pressas, apenas para ser entregue, desprovido de todas as suas funções principais.

4 CONCLUSÕES

O processo de elaboração do PIA/DPIA possui várias etapas que podem variar de acordo com a metodologia adotada ou com as recomendações da autoridade nacional respectiva. Entretanto, podemos dividi-lo em quatro eixos principais: (i) *o eixo da análise de sua*

[68] Seja a sua elaboração ou mera requisição de envio à autoridade.

necessidade; (ii) o eixo da avaliação de adequação (*compliance*), que é uma avaliação predominantemente jurídica; (iii) o eixo da avaliação de impactos e riscos; e (iv) o eixo da implementação de medidas adequadas e proporcionais para a mitigação dos impactos e riscos identificados.

No primeiro eixo, a obrigatoriedade legal do relatório nasce de tratamentos de dados que gerem altos riscos aos direitos e às liberdades fundamentais. A necessidade pode ser extraída de tratamentos de dados presumidos por lei ou regulamento a ensejar alto risco, ou em uma análise interna feita pelo controlador.

No segundo eixo, o *objeto* (projeto, sistema, tratamento, etc) da avaliação deve *enfoque* mínimo limitado. No cenário brasileiro, o *enfoque* de adequação mínimo dado ao RIPD pode ser a LGPD, somente, ou a LGPD em conjunto com outros diplomas legais que incidam sobre a atividade de tratamento (e.g. LGPD + ECA, LGPD + CDC, etc.), para que o controlador saiba se cumpriu adequadamente a sua tarefa e prossiga com a próxima etapa. Se a atividade de tratamento não possui os padrões mínimos de adequação à lei, mesmo que se avalie e mitigue os riscos, isso não sanará os vícios originários da atividade, e, portanto, descumprirá a lei diretamente. Por exemplo, não faz sentido que se proceda uma avaliação de impacto ambiental após a instalação e o funcionamento de uma fábrica, para depois adequá-la para mitigar os riscos identificados. Também não faz sentido que se proceda com uma avaliação de riscos à segurança do trabalho em determinada empreitada após a construção do edifício.

No terceiro eixo, não há limitação de *enfoque* para a avaliação dos riscos. Não se pode limitar os riscos, do ponto de vista do titular, aos riscos de proteção de dados. Tudo que puder influenciar, positiva ou negativamente, os direitos e as liberdades, deve ser levado em conta.

No quarto eixo, os riscos identificados devem ser mitigados por medidas de segurança, técnicas ou administrativas *adicionais,* suficientes para sua mitigação até um nível aceitável. Neste eixo, pode haver o controle prévio da autoridade ou não, a depender da legislação aplicável. Como vimos, no *GDPR* há esse controle quando há altos riscos residuais.

Para não relegar o RIPD à sua banalização, a ferramenta deve ser entendida como uma abordagem *escalável e proporcional* ao *compliance,* em que a identificação do elemento "alto risco", antes mesmo se proceder com detalhes sobre o projeto, e muito antes de iniciar sua implementação, para a deflagração de sua obrigatoriedade, são seus elementos centrais e in-

dissociáveis, assim como no *GDPR*, de forma a focar os esforços da ANPD para as situações críticas, antes que o dano ocorra, e também para não onerar desnecessariamente o controlador.

BIBLIOGRAFIA

Cabinet Office, Cross Government Actions: **Mandatory Minimum Measures**. 2008.

CABRAL, Filipe F. **O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais. Lei nº 13.709/18.**

CLARKE, Roger. An evaluation of privacy impact Assessment guidance documents (2011). **International Data Privacy Law**, Vol. 1, No. 2, 2011.

CLARKE, Roger. Approaches to Impact Assessment. Exhibit 1: Assessment Categories. According to Focus. **Rogerclarke**, 2014. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html#AF.

CLARKE, Roger. Privacy Impact Assessment: Its Origins and Development, Roger Clarke, **Computer Law & Security Review,** 25, 2, 2009.

CLARKE, Roger. The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR. For a Panel at CPDP, Brussels. **Rogerclarke**, 27 January 2017. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html.

DIRETIVA 95/46/EC.

EDPS. **Accountability on the ground Part I:** Records, Registers and when to do Data Protection Impact Assessments. 2018.

EDPS. **Accountability on the ground Part II:** Data Protection Impact Assessments & Prior Consultation. 2019.

General Data Protection Regulation – GDPR.

GOMES**,** Maria Cecília Oliveira. Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD. **Revista AASP**, n. 144, 2019.

GOMES, Maria Cecília Oliveira. Desafios da Regulamentação do Relatório de Impacto. **jota-info**, 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.

ICO. PRIVACY IMPACT ASSESSMENT HANDBOOK. VERSION 2. 2009. **Huntonprivacyblog.** Disponível em:

https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2013/09/PIAhandbookV2.pdf.

KLOZA, Dariusz *et al.* (2017). **Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals.**

Lei Geral de Proteção de Dados Pessoais.

PONTES DE MIRANDA, Francisco Cavalcanti. **História e Prática do Habeas Corpus**. 2. ed. José Konfino, 1955.

PRIVACY IMPACT ASSESMENT AND RISK MANAGEMENT. **Trilateral Research & Consulting,** 2013.

STURARI, Matheus. O DPIA na LGPD: interpretação nacional ou banalização do instrumento? Perfil do **Linkedin**, Publicado em 29 de outubro de 2020. Disponível em: https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpreta%C3%A7%C3%A3o-nacional-ou-banaliza%C3%A7%C3%A3o-do-matheus/.

TANCOCK, David; PEARSON,Siani; CHARLESWORTH, Andrew. **The Emergence of Privacy Impact Assessments**. 2010.

THE EU SHOULD REGULATE AI ON THE BASIS OF RIGHTS, NOT RISKS**. Access Now**, 17 de fevereiro de 2021. Disponível em: https://www.accessnow.org/eu-regulation-ai-risk-based-approach/.

WP29, "STATEMENT OF THE WP29 ON THE ROLE OF A RISK-BASED APPROACH IN DATA PROTECTION LEGAL FRAMEWORKS"**.** 2014.

WP29. 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. 2017.

ZANATTA, Rafael; A.F. **Proteção de dados pessoais como regulação de risco**: uma nova moldura teórica? (2017). Artigos Selecionados REDE 2017. I Encontro da Rede de Pesquisa em Governança da Internet.