Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos

Kloza, Dariusz; Van Dijk, Niels; Gellert, Raphaël Maurice; Borocz, Istvan Mate; Tanas, Alessia; Mantovani, Eugenio; Quinn, Paul; Rielli, Mariana

Published in:
d.pia.lab Policy Brief

Publication date:
2020

Document Version:
Final published version

Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos

d.pia.lab Documento de Política n.º 1/2017

Dariusz KLOZA, Niels VAN DIJK, Raphaël GELLERT, István BÖRÖCZ,
Alessia TANAS, Eugenio MANTOVANI e Paul QUINN
Laboratório de Avaliações de Impacto à Privacidade e à Proteção de Dados de Bruxelas (d.pia.lab)

Este documento fornece recomendações para a União Europeia (UE) que facilitam o cumprimento da exigência legal de elaboração de relatórios de Avaliação de Impacto sobre a Proteção de Dados (AIPD), conforme definido pelo Regulamento Geral de Proteção de Dados (RGPD), com o objetivo de atingir uma proteção de dados pessoais mais robusta. Em abril de 2016, a UE concluiu a parte central da reforma do seu regime jurídico de proteção de dados pessoais. A UE está, atualmente, preparando medidas e diretrizes de implementação e manuais para dar pleno efeito às novas disposições jurídicas antes da sua entrada em vigor em maio de 2018. Tal reforma introduziu, dentre outras 'novidades', uma obrigação legal de elaboração de um AIPD. Entretanto, tal exigência padece de alguns pontos fracos. De forma a remediar essas limitações e para alimentar esse processo contínuo de elaboração de políticas, este documento de política ('policy brief'[1]) busca esboçar boas práticas para um tipo genérico de avaliação de impacto, i.e., recomendado para diferentes áreas[2] (seção II). A seção III faz uma avaliação preliminar sobre como essas boas práticas se relacionam com os requerimentos específicos determinados pelo RGPD para relatórios de avaliação de impacto, i.e., *Data Protection Impact Assessment* (DPIA).

Essas seções são precedidas por informações contextuais sucintas sobre avaliações de impacto como por exemplo: definição, panorama histórico, suas vantagens e desvantagens (seção I). A Seção IV conclui com recomendações para o cumprimento da exigência de AIPDs pelo RGPD de forma a: (1) expandir o âmbito de aplicação dessa obrigação legal; (2) desenvolver métodos para a realização dessas avaliações de impacto; (3) estabelecer 'centros de referência' em AIPD nas autoridades nacionais de controle dos tratamentos de dados pessoais. Este documento de política é endereçado principalmente a formuladores de políticas públicas na União Europeia e em seus Estados-membros, sem prejuízo do potencial interesse que possa despertar nos seus pares ao redor do mundo.

1 INTRODUÇÃO

1.1 CONTEXTO

A lei de proteção de dados da União Europeia, recentemente reformada, exigirá que os responsáveis pelo tratamento[3] elaborem uma avaliação de impacto dos tratamentos de dados pessoais que sejam "susceptíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares". Esta nova exigência foi denominada como 'avaliação de impacto sobre a proteção de dados', abreviada para AIPD, e é esperado que desempenhe um papel central no sistema de proteção de direitos fundamentais na UE. A relativa novidade dessa exigência, bem como a entrada em vigor iminente do novo Regulamento, requer que as partes interessadas se adaptem rapidamente, o que tem, por consequência, gerado debates acalorados na UE. Particularmente, os formuladores de políticas e as Autoridades de Controle do Tratamento de Dados Pessoais nacionais têm-

[1] "Um policy brief é um resumo conciso de um determinado assunto, as opções de políticas para lidar com esse assunto e algumas recomendações sobre a melhor opção. É direcionado a formuladores de políticas públicas e outros indivíduos que estejam interessados em formular ou influenciar políticas." Food and Agriculture Organization, *Food Security Communications Toolkit*, Rome 2011, p. 141. (Todas as notas de rodapé são provenientes do tradutor. Todas as citações utilizadas nesta tradução são tiradas da tradução oficial para o português do Regulamento Geral de Proteção de Dados. Como o padrão europeu é o português de Portugal, algumas expressões podem ser diferentes das utilizadas no direito brasileiro.)

[2] A Lei Geral de Proteção de Dados (LGPD) trabalha com o termo "relatório de impacto à proteção de dados pessoais", conceituado no Artigo 5º, XVII, enquanto o RGPD utiliza a expressão "avaliação de impacto sobre a proteção de dados pessoais" no seu Artigo 35°.

[3] O 'responsável pelo tratamento' na LGPD é designado por 'controlador'. É um dos agentes de tratamento de dados pessoais, é aquele a que competem as decisões sobre o tratamento de dados pessoais (Artigo 5º, VI da LGPD) e em nome do qual o tratamento é realizado. No RGPD, essa figura está conceituada no Capítulo IV, Seção 1, Artigo 24° e no Artigo 4° alínea 7 que define como sendo a entidade que determina as *finalidades* e os *meios* de tratamento de dados pessoais.

 | ISSN 2565-9936

se interessado em definir a política a seguir para uma AIPD, enquanto organizações públicas e privadas têm-se focado em como cumprir essa nova obrigação legal.

1.2 HISTÓRIA

Uma avaliação de impacto é uma ferramenta usada para a análise de possíveis consequências de uma iniciativa sobre um interesse ou interesses sociais relevantes, se essa iniciativa puder apresentar perigos a esses interesses. Essa ferramenta tem o objetivo de apoiar um processo decisório informado sobre se se deve começar a iniciativa e sob quais condições, acabando por se traduzir num meio de proteção dos referidos interesses sociais.

Avaliações de risco e técnicas de avaliação semelhantes surgiram a partir da emergência de novos – e, à época, desconhecidos – perigos para questões sociais individuais e coletivas. Elas visam abordar a incerteza e o risco. Por exemplo, avaliações tecnológicas (TAs) surgiram nos anos 1960 nos Estados Unidos, inicialmente como uma ferramenta usada por cientistas para lidar melhor com as consequências potencialmente perigosas de descobertas e invenções. Elas foram subsequentemente institucionalizadas como uma forma de garantir – inicialmente – segurança de produtos e foram progressivamente abrangendo um espectro mais amplo de problemas relacionados à sociedade e à tecnologia. Similarmente, avaliações de impacto ambiental (AIAs) surgiram como uma resposta à gradual degradação do meio ambiente. Experiências positivas com ambas as avaliações auxiliaram a sua disseminação como prática ao redor do mundo e resultaram na proliferação e, às vezes, na institucionalização, de avaliações de impacto em áreas que incluem a saúde, regulação (governança)[4], segurança nacional, práticas de vigilância[5] e, também, privacidade e proteção de dados pessoais.

A proliferação de Avaliações de Impacto à Privacidade (AIPs) e sobre a Proteção de Dados (AIPDs) é atribuída a três fatores principais: (1) o caráter crescentemente invasivo de tecnologias emergentes sobre as vidas dos indivíduos e sobre o tecido social; (2) a crescente importância do tratamento de dados pessoais para a economia contemporânea, segurança nacional, pesquisa científica, desenvolvimento tecnológico, relações interpessoais, dentre outros, e (3) a diminuição da confiança em tecnologias emergentes e a sua utilização por entidades públicas e privadas. Não obstante, cerca de 50 anos após o surgimento das avaliações de impacto, elas ainda não constituem uma prática clara. Apenas em certas áreas ganharam considerável experiência e maturidade (e.g. ambiental). Em outras, suas identidades ainda estão sendo desenvolvidas (e.g. relatório de impacto 'social' e AIPDs) e, em outras, ainda, clama-se constantemente por sua introdução (e.g. direitos humanos).

As Avaliações de Impacto à Privacidade (AIP) (*Privacy Impact Assessment*, PIA) – e subsequentemente as Avaliações de Impacto sobre a Proteção de Dados (*Data Protection Impact Assessment*, DPIA) – emergiram nos anos 1990 e foram institucionalizadas, de diferentes maneiras e com vários níveis de compulsoriedade, primeiro em jurisdições de *common law*, como Nova Zelândia, Austrália e Canadá. Na Europa, a primeira política para PIA foi desenvolvida no Reino Unido em 2007. A UE desde então desenvolveu duas políticas de PIA voluntárias para setores específicos: a primeira para aplicações de identificação por radiofrequência (IDRF) (2009) e a segunda para 'redes elétricas inteligentes' (2012). No Programa para Legislar Melhor (*Better Regulation Package*, 2015), a privacidade e a proteção de dados pessoais constituem um de muitos objetos de avaliação nas leis e elaborações de políticas da UE. Com a adoção do RGPD e da Diretiva sobre a Proteção de Dados na Aplicação da Lei (*Data Protection Law Enforcement Directive*, 2016), uma política obrigatória para a avaliação de impacto vai ser instituída na UE pela primeira vez, em maio de 2018, na área da proteção de dados pessoais. Não se trata de um movimento solitário, na medida em que a modernização recentemente finalizada da Convenção 108 do Conselho da Europa[6] e a nova lei de proteção de dados proposta na Suíça (se adotada em sua redação atual) introduzirão uma política semelhante.

1.3 VANTAGENS

As vantagens na realização de avaliações de impacto encontram-se predominantemente na sua contribuição para (1) a tomada de decisões informadas e (2) a proteção de interesses sociais. A primeira categoria normalmente atrai organizações públicas e privadas, trazendo os benefícios da mudança para um pensamento antecipado e *ex ante*. Essas organizações tornam-se capazes de refletir sobre as consequências das iniciativas vislumbradas, assim como os meios para minimizar ou eventualmente até evitar consequências negativas e não intencionais antes que elas ocorram (i.e., um 'sistema de alerta precoce'), o que traz ganhos em termos de recursos e de confiança pública. Além disso, as avaliações de impacto podem facilitar a conformidade com requerimentos legais e regulatórios em geral (e.g. padrões técnicos e *standards*). Sendo uma

[4] Acerca de relatório de impacto por órgãos reguladores enquanto medida de governança, destaca-se que recentemente a Lei de Introdução às Normas do Direito Brasileiro (LINDB) passou por um processo de reforma e dentre os dispositivos mais discutidos esteve o Artigo 20°, que prevê que em todas as esferas, "não se decidirá com base em valores jurídicos abstratos sem que sejam consideradas as consequências práticas da decisão". Tal previsão corresponde a ideia de um relatório de impacto genérico que será discutida neste documento.

[5] No caso brasileiro, as atividades de tratamento de dados para fins de vigilância nos contextos de segurança pública, defesa nacional e persecução criminal foram excluídas do escopo de aplicação da LGPD. Não obstante, o mesmo dispositivo, no parágrafo 3º, prevê que "A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais."

[6] Tal obrigação está disposta no Artigo 10° da Convenção Modernizada: "2. *Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms*." Vale destacar que o Brasil, desde 2018, integra a Convenção na qualidade de observador.

obrigação de 'melhores esforços'[7], elas constituem evidência de *due diligence*, o que poderia reduzir ou eventualmente até eliminar a responsabilidade civil. Também demonstrariam *accountability*[8] em relação a autoridades reguladoras, que, de sua parte, teriam seu trabalho facilitado. Eventualmente, avaliações de impacto, se conduzidas de uma maneira transparente, reforçariam a confiança pública, demonstrando que uma organização leva questões sociais a sério; o setor privado comumente utiliza avaliações de impacto para demonstrar responsabilidade social corporativa.

A segunda categoria normalmente atrai governos, pois as avaliações de impacto auxiliam o cumprimento da sua missão de oferecer proteção, de forma prática e eficiente, a interesses sociais relevantes (e.g. certos direitos humanos, como a privacidade) em benefício dos indivíduos e da sociedade como um todo. Para os indivíduos, as avaliações de impacto são um meio para vocalizar suas preocupações (e.g. por meio de participação social), o que fortaleceria uma ideia de devido processo legal. As avaliações de impacto buscam acomodar interesses diversos e consequentemente contribuem com o desenho de uma 'tênue linha vermelha' entre interesses igualmente legítimos, mas aparentemente concorrentes, como segurança nacional e proteção de dados pessoais (e.g. no caso de AIPD) ou a competitividade da economia nacional e a proteção do meio ambiente (e.g. no caso de avaliação de impacto ambiental). Em comparação com outras ferramentas de proteção, as avaliações de impacto oferecem um escopo mais amplo de proteção do que, por exemplo, testes de conformidade, que podem ser facilmente reduzidos a meros exercícios de *check-list*.

1.4 DESVANTAGENS

Críticos têm argumentado que as avaliações de impacto constituem uma carga desnecessária, aumentando uma burocracia já superdimensionada, causando gastos supérfluos e atrasos na tomada de decisões, ou mesmo retardando todo o processo de inovação (não é, portanto, surpresa que haja um desejo recorrente que avaliações de impacto sejam rápidas, simples e baratas). Oponentes enfatizam a complexidade do processo de avaliação na prática, as dificuldades que ele traz, juntamente com a falta de experiência prática, e orientação e supervisão mínimas ou inexistentes. Questiona-se, também, a mais-valia da avaliação de impacto em relação a outras técnicas, como a verificação de conformidade, bem como sua eficácia, salientando a ampla discricionariedade geralmente conferida sobre a forma de condução de avaliações de impacto e até mesmo sobre se elas devem ser realizadas ou não.

As avaliações de impacto são comumente criticadas por sua aparente natureza de 'palavras vazias', sendo utilizadas exclusivamente para cumprir uma exigência regulatória, por sua condução com o mínimo esforço, ou por seu emprego instrumental, unicamente para legitimar iniciativas intrusivas. Além disso, as organizações às vezes focam-se na condução de avaliações *in abstracto* ao invés de utilizá-las como um meio para de fato abordar o impacto das suas iniciativas. Elas frequentemente confundem avaliações de impacto com auditorias. As organizações consideram, erroneamente, apenas as consequências que se relacionam com elas próprias (e.g. riscos financeiros ou reputacionais), ao invés de avaliar também as consequências para os indivíduos e o público em geral. Em última análise, avaliações de impacto são frequentemente realizadas tarde demais, por exemplo, quando o projeto de uma iniciativa não pode mais ser influenciado significativamente. Críticos ainda sugerem que, quando as avaliações de impacto são compulsórias, elas representam uma exigência regulatória muito restrita em seu escopo, permitindo que iniciativas que apresentam um perigo significativo escapem ao escrutínio. Ademais, quando as avaliações de impacto são realizadas, elas normalmente apresentam falhas de transparência, i.e., o processo como um todo é opaco, difícil de entender por uma pessoa leiga (devido ao alto nível de complexidade técnica), sendo difícil, ou quase impossível, encontrar os resultados finais ou as recomendações. Elas frequentemente falham também na inclusão de participação pública ou dão a ela um escopo muito limitado, tornando a participação desprovida de sentido.

II. BOAS PRÁTICAS PARA AVALIAÇÃO DE IMPACTO

A partir de uma análise comparativa de avaliações de impacto em múltiplas áreas, tentaremos esboçar os elementos que constituem boas práticas para uma versão genérica de avaliação de impacto, isto é, recomendada para diferentes áreas. Este exercício servirá para avaliar o requerimento legal de AIPD no RGPD na seção subsequente.

1. A avaliação de impacto deve ser um processo sistemático, conduzido de acordo com um método apropriado e em tempo hábil. Deve ser iniciada razoavelmente cedo no ciclo de vida de uma iniciativa específica, ou de algumas iniciativas semelhantes (e.g. uma tecnologia proposta ou um projeto de lei), antes de sua implementação, e continuar acompanhando o seu ciclo de vida – à medida que a sociedade muda, os riscos evoluem e o conhecimento cresce –, sendo revisitada quando necessário (um 'instrumento vivo'), influenciando continuamente a concepção da iniciativa em avaliação.

[7] É possível associar a ideia de 'melhores esforços' aqui empregada ao conceito, do direito brasileiro, de obrigação de meio. Diferente da obrigação de resultado, em que uma entrega concreta e pré-determinada é devida, na obrigação de meio o devedor se compromete a empreender seus melhores esforços para a obtenção de determinado resultado. Embora a AIPD, no RGPD, seja compulsório em determinados casos, é evidente que sempre haverá um risco residual, maior ou menor, após a sua realização, de forma que se pode falar que o controlador deve empregar 'melhores esforços' para alcançar uma situação em que o risco seja o menor possível, sabendo-se que ele nunca será nulo.

[8] Relevante destacar que tanto a LGPD, no Artigo 6º, X, quanto o RGPD, no Artigo 5° n°2 elencam a accountability como princípio de proteção de dados pessoais. No caso brasileiro, optou-se por traduzir o termo '*accountability*' como responsabilidade e prestação de contas, o que evidencia o caráter duplo deste princípio – não basta estar em conformidade com as exigências regulatórias, mas é necessário desenvolver meios adequados para demonstrar tal conformidade.

2. As avaliações de impacto devem analisar as possíveis consequências de uma iniciativa relativamente aos interesses sociais relevantes, tanto individuais quanto coletivos, proporcionalmente ao seu tipo (e.g. AIPD diz respeito à proteção de indivíduos sempre que seus dados estejam sendo tratados e AIA diz respeito ao ambiente natural e humano). Análises de limiar (triagem, análise de contexto), participação pública e consulta a especialistas ajudam a determinar e atualizar a lista destes interesses sociais. Sempre que necessário, múltiplos tipos de avaliação de impacto são realizados para uma dada iniciativa, possivelmente de maneira integrada.

3. Nem todas as iniciativas requerem avaliações de impacto. A necessidade é determinada por fatores tais como a natureza, o âmbito, o contexto e a finalidade da iniciativa a ser avaliada, bem como do número e tipos de indivíduos afetados etc. As avaliações de impacto são, no entanto, obrigatórias no caso de iniciativas capazes de causar consequências negativas severas para os interesses sociais relevantes.

4. Não existe um método infalível ou 'à prova de balas' para a condução de avaliações de impacto. O que importa é a escolha de um método de avaliação apropriado que permita o melhor entendimento e tratamento das possíveis consequências da iniciativa em causa. Esses métodos podem variar entre o gerenciamento de riscos qualitativo ou quantitativo, o planejamento de cenários, ou a previsão científica, apoiados por uma verificação de conformidade com requisitos legais e regulamentares relevantes (e.g. padrões técnicos).

5. O processo de avaliação de impacto identifica, descreve e analisa as possíveis consequências – positivas ou negativas, pretendidas ou não pretendidas – de uma iniciativa sob avaliação, mas também identifica, descreve e analisa possíveis soluções (recomendações) para abordar essas consequências.

6. As avaliações de impacto constituem obrigações de 'melhores esforços'[9]. Já que é impossível reduzir consequências negativas ou maximizar as positivas em termos absolutos, as organizações reagem a elas da melhor forma possível, dependendo das técnicas mais avançadas e, em uma medida razoável, dos recursos disponíveis.

7. O processo de avaliação de impacto requer que o avaliador, ou a equipe de avaliadores, tenha conhecimento e *know-how* suficientes para sua conclusão bem-sucedida, a depender do tipo de avaliação de impacto sob apreciação.

8. O processo de avaliação de impacto é documentado (por escrito, particularmente) e é razoavelmente transparente. Sua transparência se manifesta no livre (i.e., irrestrito) e público acesso a informações relevantes. O público em geral é informado sobre o processo de avaliação, seus termos de referência (o método, em particular) e seu progresso. Tanto o esboço quanto o relatório final de avaliação são facilmente acessíveis. Isso não prejudica o segredo de empresa.

9. O processo de avaliação de impacto é deliberativo, o que se manifesta predominantemente pela participação pública. Atores externos – sejam indivíduos e/ou organizações da sociedade civil preocupados ou afetados pela iniciativa sob avaliação, na forma mais representativa possível – são identificados e informados sobre ele, sua voz é ativamente buscada e devidamente levada em consideração (i.e., consulta e co-decisão). Informações fornecidas e buscadas são robustas, precisas e inclusivas. Os indivíduos e/ou os seus representantes têm meios efetivos de impugnar o processo, e.g. em um Tribunal ou arena semelhante. Paralelamente, qualquer um dentro da organização que patrocina a iniciativa sob avaliação (i.e., atores internos) participa do processo nas mesmas condições. Exceções à inclusão de participação pública, quando justificadas, são interpretadas restritivamente.

10. Uma organização que patrocina uma iniciativa é responsável[10] pelo processo de avaliação de impacto. Os tomadores de decisão dentro de uma organização escolhem, *inter alia*, o método de avaliação, bem como os avaliadores que o conduzirão. Eles eventualmente aprovam o relatório final da avaliação de impacto e, subsequentemente, monitoram a implementação de possíveis soluções propostas (recomendações). Uma entidade externa (e.g. uma autoridade reguladora ou um órgão de auditoria) escrutina sua qualidade; os critérios de seleção são transparentes. Dessa forma, a organização é capaz de demonstrar a satisfatoriedade do processo de avaliação de impacto empreendido. Sempre que as avaliações de impacto forem compulsórias, a não-conformidade e a negligência serão sancionadas proporcionalmente.

11. A independência do avaliador – seja externo ou interno (*in-house*) – é garantida: ele não busca ou recebe nenhuma ordem, e tem recursos suficientes (i.e., tempo, dinheiro, mão de obra, conhecimento e *know-how*, local e infraestrutura) à sua disposição.

12. O processo de avaliação de impacto é suficientemente simples, ou seja, não é indevidamente oneroso. O método serve aqueles que o utilizam e é, portanto, estruturado, coerente, facilmente compreensível, além de evitar ser demasiadamente prescritivo, complexo ou causar utulização abusiva de recursos. Existe um *trade-off* entre a simplicidade e a sofisticação técnica e exatidão da avaliação.

13. O processo de avaliação de impacto se adapta às características da iniciativa sob avaliação e a organização que a patrocina (isto é, não há um padrão único compatível com todos os modelos de organização), por exemplo tipo e complexidade (e.g. desenvolvimento tecnológico, pesquisa científica, propostas legislativas) ou o tipo e número de indivíduos atingidos (e.g. segurança nuclear não é igual a proteção de dados pessoais). Ela pode ser conectada com avaliações de impacto em outras áreas, se possível. É sensível a diferenças culturais e geográficas.

[9] Vide Nota 7.
[10] Conforme Nota 8, destaca-se que a accountability inclui também a prestação de contas, para além da responsabilidade.

14. O processo de avaliação de impacto é inclusivo. Isso garante que o máximo possível de atores, interesses sociais relevantes e fases de desenvolvimento relevantes (ou seja, tanto a iniciativa sob análise quanto o processo que levou a ela) – proporcionais às questões sociais em jogo e ao tipo de avaliação – sejam incluídos no processo de avaliação. Ele baseia sua análise tanto em conhecimento especializado quanto leigo (e.g. participação pública).

15. A avaliação de impacto é receptiva. Tanto o método quanto o processo evoluem aprendendo com experiências prévias de técnicas de avaliação semelhantes (e.g. TA, AIA, gerenciamento de riscos etc.), conhecimento de disciplinas correlatas (e.g. direito) e mudanças na sociedade.

16. Avaliações de impacto requerem um ambiente favorável para dar frutos. Elas exigem o apoio contínuo do mais alto nível de tomadores de decisão, bem como um espírito colaborativo entre atores externos e internos. Os reguladores oferecem orientações e assistência prática no processo de avaliação, na forma de treinamentos, manuais, explicações e conselhos adequados.

DISPOSIÇÕES RELEVANGTES DO RGPD

- "Quando um certo tipo de tratamento … for susceptível de implicar um elevado risco para os direitos e liberdades de pessoas singulares, o responsável pelo tratamento procede … a uma avaliação …" (Artigo 35° n.°1)
- "A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados" (Artigo 35° n.°4)
- "A avaliação inclui, pelo menos … as medidas previstas para fazer face aos riscos … tendo em conta os direitos e legítimos interesses dos titulares de dados e outras pessoas em causa" (Artigo 35° n.°7 al. d)
- "Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto …" (Artigo 35° n.°9)
- "As violações das disposições [… estão] sujeitas a coimas até 10 000 000 EUR …" (Artigo 83° n.°4)

III. AVALIAÇÃO DOS REQUISITOS LEGAIS DA AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS NO RGPD

Avaliaremos, agora, um tipo específico de avaliação de impacto, a AIPD, conforme prescrito pelo Artigo 35° do RGPD, à luz das boas práticas descritas na seção anterior para um tipo genérico de avaliação de impacto. Daremos ênfase particular a algumas especificidades da nova lei de dados pessoais da UE que são consideradas chave, i.e o princípio de *accountability*, o 'gancho legal' para AIPD e a 'abordagem baseada em riscos'.

1. O RGPD, no âmbito da sua aplicação, torna compulsório que os responsáveis pelo tratamento, com o auxílio do subcontratante (se aplicável), elaborem uma AIPD para tipos de tratamento susceptíveis "de implicar um elevado risco para os direitos e liberdades de pessoas singulares". A falha no cumprimento deste requisito resulta em sanções severas. Dessa forma, o RGPD desloca a atenção de medidas reativas para outras mais proativas.

2. Ao requerer que os responsáveis pelo tratamento de dados realizem uma AIPD "antes de iniciar o tratamento [de dados pessoais]" e, subsequentemente, que revejam suas avaliações nos casos em que os riscos e/ou as operações de tratamento tenham mudado, o RGPD indica que a AIPD é um processo sistemático e um 'instrumento vivo'.

3. O âmbito do requisito legal para a realização de uma AIPD segue o âmbito do RGPD: protege-se o direito fundamental à proteção de dados pessoais assim como outros direitos e liberdades fundamentais afetados pelo tratamento de dados pessoais. O RGPD não se aplica ao tratamento de dados anônimos, de modo que o escopo da proteção não é completo.

4. O RGPD requer uma AIPD apenas em casos de "elevado risco". Isso limita seu âmbito para alguns tipos de operações de tratamento de dados. As Autoridades de Controle do Tratamento de Dados nacionais podem expandir este catálogo, mas também podem restringi-lo. Não obstante, como o RGPD confere um nível de proteção mais elevado a dados sensíveis e a dados sobre os registros criminais, isso foi refletido no âmbito do requisito legal para a realização de uma AIPD.

5. O RGPD aproxima os conceitos de 'risco' e 'direito', que tradicionalmente pertencem a esferas do conhecimento e organização social muito diferentes. Direitos são tipicamente definidos e refinados em Tribunais por meio de conceitos jurídicos, geralmente de forma retroativa após uma suposta infração à lei. O conceito de risco pertence às práticas de gerenciamento de risco dentro de organizações, geralmente definidas por meio de conceitos científicos de probabilidade, na tentativa de prospectivamente lidar com possíveis consequências futuras. Esta fusão cria um objeto de avaliação novo para o qual ainda não há um método comum definido.

6. O RGPD trouxe ao campo da proteção de dados terminologias de gerenciamento de risco, como 'elevado risco', 'probabilidade', 'impacto' e 'severidade'. Não é claro, no entanto, o que esses termos significam no contexto de proteção

de dados, ou – mais amplamente – de "direitos e liberdades de pessoas singulares"[11]. Vários destes termos podem não ser diretamente relevantes, ou sejam difíceis de conciliar, com o direito europeu de proteção de dados e podem gerar complicações artificiais para o processo de avaliação. Como resultado, muitos deles deverão receber um novo significado autônomo.

7. O RGPD conecta a AIPD à necessidade de consultas prévias caso o processo de avaliação indique riscos residuais de elevado nível. Dessa forma, confere-se amplos poderes às Autoridades de Controle sobre o Tratamento de Dados nacionais, que podem fornecer orientações por escrito e – caso mais medidas sejam necessárias – podem, inclusive, proibir as operações de tratamento de dados vislumbradas.

8. O RGPD fornece critérios para quando uma AIPD deve ser realizada. Ela oferece, entretanto, poucas indicações sobre o processo em si e é silente sobre questões metodológicas. Essa abordagem minimalista pretende constituir um 'gancho legal' para ser complementado por métodos específicos para conduzir uma AIPD, todavia, certos elementos centrais permanecem sem resposta.

9. O RGPD requer, durante o processo de AIPD, que o responsável pelo tratamento consulte os titulares dos dados ou os seus representantes, com a devida observância de segredo industrial ou empresarial. Entretanto, este requisito é comparativamente fraco, já que só é acionado "quando apropriado", dizendo respeito apenas a titulares de dados (e não ao público, em geral), e o RGPD não dá nenhuma indicação de quando isso deve ocorrer. Ela também falha em especificar quem exatamente deve ser consultado, como identificar esses indivíduos, quando se pode recorrer a representantes, o que é considerado uma representatividade legítima, bem como quais são meios de contestação disponíveis.

10. O RGPD fica silente quanto à transparência do processo de AIPD. Particularmente, não há um requerimento para que o esboço e o relatório final ou um resumo dele sejam publicados.

11. Há um requerimento vago para que o European Data Protection Board (EDPB)[12] emita diretrizes para "assegurar a aplicação coerente do Regulamento", e o desenvolvimento e atualização de métodos para uma AIPD pode cair no âmbito deste objetivo. Apenas após a sua emissão será possível avaliar esses métodos.

12. O RGPD dá aos responsáveis pelo tratamento alguma discricionariedade na realização de uma AIPD, em pelo menos dois aspectos: primeiro, na determinação sobre se as operações de tratamento se enquadram no critério pré-definido de elevado risco; segundo, se os riscos residuais são suficientemente elevados para gerar a obrigação de consulta à Autoridade de Controle sobre o Tratamento de Dados. Além disso, pela própria natureza do processo de gerenciamento de risco, os responsáveis pelo tratamento escolhem, *inter alia*, o método de avaliação e as medidas de mitigação de riscos. Também cabe aos responsáveis pelo tratamento escolher avaliadores qualificados e garantir a sua independência, assegurar a robustez do processo como um todo, e documentá-lo apropriadamente. Os responsáveis pelo tratamento são integralmente responsáveis por estas escolhas metodológicas.

13. Está implícito que o RGPD reconhece as diferenças culturais e geográficas na proteção de dados pessoais. Em particular, exceções nacionais relacionadas a, por exemplo, a liberdade de expressão, devem ser levadas em consideração no processo de avaliação.

14. O RGPD é silente em relação aos papéis e responsabilidades para a condução de uma AIPD. Particularmente, o papel do encarregado de proteção de dados (*data protection officer*) é incerto. O RGPD requer apenas que ele aconselhe o avaliador no processo de avaliação, mas sem nenhuma especificidade.

IV. RECOMENDAÇÕES

A avaliação exposta demonstrou que o requerimento de AIPD do RGPD satisfaz alguns dos elementos de boas práticas para relatórios de impacto, mas falha em outros aspectos. Portanto, oferecemos agora recomendações para os responsáveis pela elaboração de políticas públicas europeias com o objetivo de 'fechar essa lacuna'. Estas recomendações têm três vertentes: primeiro, sugerimos o alargamento do âmbito do requisito para a realização de uma AIPD. Subsequentemente, propomos o desenvolvimento de múltiplos métodos para que uma AIPD possa abordar as omissões e falhas do Artigo 35° do RGPD. Por fim, sugerimos que tanto o *European Data Protection Board* quanto as Autoridades de Controle sobre o Tratamento de Dados nacionais tomem a iniciativa e tornem-se 'centros de referência' em AIPD. Os autores também são realistas em relação à probabilidade de que as suas recomendações sejam, de fato, implementadas, i.e., estas recomendações dependem dos poderes normativo e consultivo que o RGPD concede tanto ao EDPB quanto às autoridades nacionais e regionais de proteção de dados.

[11] O contexto normativo brasileiro traz desafios ainda maiores quando se considera que não há nem uma mínima procedimentalização do relatório de impacto à proteção de dados pessoais na lei, de maneira que caberá à Autoridade Nacional de Proteção de Dados todo o ônus de determinar parâmetros para sua efetivação na prática.

[12] O processo aqui mencionado já está acontecendo. As Autoridades de Controle sobre o Tratamento de Dados (DPAs) dos países-membros da UE elaboraram listas individuais, chamadas '*white lists*', para tratar de atividades que não requerem uma AIPD e '*blacklists*' para atividades que devem ser precedidas pelo relatório, cf.: https://iapp.org/resources/article/eu-member-state-DPIA-whitelists-and-blacklists. Posteriormente, o EDPB emitiu uma opinião para cada uma das listas, com o objetivo de uniformizar o entendimento em torno da necessidade de efectuar uma AIPD, cf.: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

A. Âmbito

1. A lista de operações de tratamento de dados que se inserem no âmbito do requisito legal para a realização de uma AIPD deve ser alargada para que as operações intrusivas não escapem ao seu escrutínio. Essa lista deve ser mantida atualizada.
2. Sempre que iniciativas intrusivas caírem fora do âmbito do requisito legal da AIPD do RGPD, é recomendado recorrer a outros tipos de avaliação, e.g. relatórios de impacto à privacidade.

B. Métodos

3. O EDPB[13] está melhor posicionado para emitir e manter atualizados métodos para a condução de AIPD para toda a Europa. As autoridades nacionais e regionais, por sua vez, estão melhor posicionadas para ajustá-los aos seus contextos locais, sempre respeitando as regras de harmonização do RGPD. Devido à relativa novidade do requerimento de AIPD, estes métodos devem ser desenvolvidos com cautela.
4. Estes métodos devem ser adaptáveis:
    a. Devem existir múltiplos métodos para a condução de AIPD, adaptados para refletir a diversidade dos setores da indústria ou governo e os riscos específicos ligados a cada um. Estes métodos devem respeitar diferenças jurídicas, culturais, sociais ou éticas em múltiplas jurisdições;
    b. Eles devem ser revisados periodicamente conforme a experiência de condução de AIPDs cresce e os contextos sociais mudam.
5. Estes métodos devem endereçar, particularmente:
    a. Condições para participação pública (i.e., identificação de atores, inclusive titulares de dados; provisão de informações; meios para ouvir diferentes vozes e levá-las em consideração; e meios para contestação);
    b. Condições para documentação e transparência (i.e., documentação escrita, acessibilidade a informações relacionadas a AIPD, registros públicos de AIPD realizados, segredo de empresa, etc.);
    c. Esclarecimentos de terminologias vagas, especialmente termos quantitativos (e.g. 'larga escala') e termos relacionados com o risco (e.g. 'risco a um direito', 'elevado risco' e 'probabilidade');
    d. Esclarecimentos quanto às qualificações e independência do avaliador;
    e. Esclarecimentos quanto aos papéis, responsabilidades e *accountability* dos atores envolvidos no processo de AIPD, particularmente responsáveis pelo tratamento, subcontratantes e encarregados de proteção de dados (DPOs).
6. Os métodos devem ser receptivos às experiências de avaliações de impacto prévias e às lições que elas têm a oferecer. Mais especificamente, lições jurídicas sobre substância e procedimentos devem ser levadas em consideração para tornar a AIPD uma ferramenta de avaliação discreta. Lições de procedimento dizem respeito ao acesso público a informações relevantes, consultas públicas e possibilidades de contestação. Lições substantivas referem-se a critérios para identificação de riscos (a serem retiradas e.g. de leis de proteção de dados), diferentes tipos de risco (direito ambiental), novos tipos de danos ou impactos (responsabilidade civil) ou níveis de probabilidade (direito baseado em evidências).
7. Condições de fiscalização (auditorias) do processo de AIPD por autoridades nacionais devem ser definidas, indo de critérios baseados em processos (e.g. a qualidade da AIPD) para critérios baseados em atores (e.g. a discricionariedade conferida aos responsáveis pelo tratamento).

C. Conhecimento e know-how

8. Tanto o EDPB quanto as Autoridades de Controle sobre o Tratamento de Dados nacionais e regionais devem estabelecer e manter 'centros de referência' com conhecimento e *know-how* relevante em AIPD. Estes centros devem cooperar uns com os outros e se tornar parte de uma comunidade mais ampla de avaliação de impacto, colaborando com associações e/ou realizando conferências dedicadas ao tema.

Em suma, as AIPDs são apenas um auxílio no processo decisório. Essas avaliações de impacto não são soluções 'à prova de balas': a qualidade da proteção que elas podem oferecer depende da forma como os responsáveis pelo tratamento e os subcontratantes as usam, do apoio que eles recebem dos formuladores de políticas e – eventualmente – da supervisão de autoridades de controle e tribunais. As avaliações de impacto não são sem dificuldades, mas com ações honestas e com métodos disponíveis, suplementados por diretrizes, conselhos e supervisão, elas podem, em última instância, contribuir para uma proteção de dados pessoais mais robusta.

---

[13] Vide Nota 13.

FONTES RELEVANTES SELECIONADAS

Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review* 25, no. 2 (2009): 123–135, doi:10.1016/j.clsr.2009.02.002.

David Wright and Paul De Hert (eds.), *Privacy Impact Assessment* (Dordrecht: Springer, 2012), doi: 10.1007/978-94-007-2543-0.

Dariusz Kloza, Niels van Dijk, and Paul De Hert, "Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies," in *Smart Grid Security*, ed. Florian Skopik and Paul Smith (Waltham, MA: Elsevier, 2015), 11–47, doi:10,1016/B978-0-12-802122-4,00002-X.

Niels van Dijk, Raphaël Gellert, and Kjetil Rommetveit, "A Risk to a Right? Beyond Data Protection Risk Assessments," *Computer Law & Security Review* 32, no. 2 (2016): 286–306, doi:10.1016/j.clsr.2015.12.017.

Raphaël Gellert, "We have always managed risks in data protection law: understanding the similarities and differences between the rights-based and the risk-based approaches to data protection," *European Data Protection Law Review* 2, no. 4 (2016): 481–492, doi:10.21552/EDPL/2016/4/7.

István Böröcz, "Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras," *European Data Protection Law Review* 2, no. 4 (2016): 467–480, doi:10.21552/EDPL/2016/4/6.

SOBRE O D.PIA.LAB

O **Laboratório de Avaliações de Impacto à Privacidade e à Proteção de Dados de Bruxelas**, ou **d.pia.lab**, conecta pesquisa básica, metodológica e aplicada, oferece treinamentos e fornece assessoramento sobre políticas relacionadas a avaliações de impacto nas áreas de inovação e desenvolvimento tecnológico. Apesar de os aspectos jurídicos da privacidade e proteção de dados pessoais constituírem o nosso foco principal, o Laboratório inclui outras disciplinas como ética, filosofia, estudos sobre vigilância e estudos na área de ciências, tecnologia e sociedade. Criado em novembro de 2015, o Laboratório constitui parte, e se baseia na experiência, do Grupo de Pesquisa em Direito, Ciência, Tecnologia e Sociedade (LSTS) da Vrije Universiteit Brussel (VUB; Universidade Livre de Bruxelas), Bélgica.

O Laboratório desenvolveu seu conhecimento baseado em avaliações de impacto provenientes de múltiplos projetos, concluídos e em andamento, como PIAF, ADVISE, EPINET, MATHISIS, FORENSOR, CANDID (co-financiados pela UE), PARENT (co-financiado pela UE e Innoviris), assim como "Um Risco para um Direito? Explorando uma nova noção em leis de proteção de dados" e "Design de Direitos: a Reconstituição Tecnológica da Privacidade e Proteção de Dados" (financiado por Fonds Wetenschappelijk Onderzoek – Vlaanderen). A visão expressa neste documento de política não reflete as visões de nenhuma destas agências de financiamento.

Nós agradecemos aos seguintes membros da rede d.pia.lab pelos seus comentários em uma versão anterior deste documento de política: Brendan van Alsenoy, Roger Clarke, Kjetil Rommetveit e Claudia Quelle. Agradecemos Pradeepan Sarma pela edição de texto.

dpialab.org | **dpialab@vub.ac.be**

SOBRE O DATA PRIVACY BRASIL (ENTIDADE PARCEIRA DA TRADUÇÃO)

O **Data Privacy Brasil** é um centro de produção e difusão de conhecimento que tem como objetivo criar, analisar e compartilhar conteúdo sobre o impacto das tecnologias da informação e comunicação (TICs) sobre a privacidade e proteção de dados pessoais, a fim de subsidiar o debate público sobre os desafios de uma sociedade e economia cada vez mais movida e orientada por dados. Para concretizar esses fins, atualmente o Data Privacy (i) oferece cursos e *workshops* sobre aspectos teóricos e práticos relativos à privacidade e proteção de dados, com especial foco na Lei Geral brasileira de Proteção de Dados (LGPD) e sua relação com normativas diversas vigentes no ordenamento jurídico brasileiro e em outras jurisdições (e.g. Regulamento Europeu de Proteção de Dados Pessoais); (ii) promove palestras, reuniões, seminários e outros eventos a fim de reunir especialistas em privacidade e proteção de dados (e temas correlatos) e suscitar avanços no debate sobre o assunto no Brasil, além de propiciar sua difusão para um público mais amplo; (iii) reúne, produz e contribui com a produção de pesquisa aplicada e conteúdo diverso, como ensaios, análises, estudos e artigos científicos.

dataprivacy.com.br | **contato@dataprivacy.com.br**