# Relatório de impacto à proteção de dados.

Uma breve análise da sua definição e papel na LGPD.

**Maria Cecília Oliveira Gomes**
É pesquisadora e líder de projeto em proteção de dados no Centro de Ensino e Pesquisa em Inovação (Cepi) da FGV Direito SP. Foi *visiting researcher* no European Data Protection Supervisor (EDPS). É pós-graduada em Propriedade Intelectual e Novos Negócios pela FGV. Seu campo de pesquisa é direcionado para o desenvolvimento de metodologias e *design* para *impact assessment*, e avaliação de risco em processos de conformidade.

**Sumário**

**1.** Introdução
**2.** Relatório de impacto à proteção de dados na LGPD
**2.1.** Origem: de onde vieram os relatórios?
**2.2.** Afinal, o que é o relatório de impacto?
**2.3.** Qual é o papel do relatório de impacto?
**3.** Conclusão
Bibliografia

## 1 Introdução[1]

No dia 14 de agosto de 2018, foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, Lei nº 13.709/2018. Tendo uma aplicação transversal, ou seja, que transpassa por todos os setores (academia, setor privado, Poder Público e terceiro setor), ela se aplica a todos (titulares de dados[2] e agentes de tratamento[3]), cabendo a estes últimos a necessidade de adequar suas operações de tratamento de dados à nova regulação.

Com exceção de alguns setores altamente regulados em proteção de dados no país, como os setores financeiro e de saúde, por exemplo, o Brasil ainda não tinha se deparado com a missão

**1.** Agradeço aos comentários da Andressa Bizutti e da Thaís Zappelini durante a elaboração deste texto.

**2.** BRASIL. Lei nº 13.709/2018. Art. 5º, inciso V: "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

**3.** BRASIL. Lei nº 13.709/2018. Art. 5º, inciso IX: "o controlador e o operador".

de adequar todos a uma nova e ampla regulação sobre o tema. Parte significativa da compreensão da necessidade de uma adequação regulatória em proteção de dados vem do papel ativo que uma Autoridade Nacional de Proteção de Dados (ANPD) deve exercer sobre o tema, elaborando orientações sobre o que é e como fazer uma adequação de atividades de tratamento à lei e indicando as ferramentas necessárias para a realização desse processo.

Contudo, no Brasil vivemos em um momento atípico, no qual há uma lei geral de proteção de dados aprovada sem uma autoridade constituída e madura que emita orientações sobre como fazer esse processo de adequação. Faltando menos de um ano para entrada em vigor da LGPD em agosto de 2020 e considerando que a ANPD ainda está em formação, fica a grande dúvida sobre como deve ser realizado o processo de conformidade com a LGPD e, mais ainda, sobre como demonstrar conformidade com a lei.

Olhando por uma perspectiva regulatória, parte da compreensão sobre como fazer um processo de conformidade, que nada mais é do que uma adequação de atividades em relação a uma regulação, é entender quais são as ferramentas disponíveis na lei que possibilitam fazer isso.

Por essa razão, 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. Uma das ferramentas que a LGPD aponta como um indicador demonstrativo de conformidade à lei é o relatório de impacto à proteção de dados[4] e, nela, através de uma análise sistemática, também é possível ter instruções sobre como manuseá-lo.

Outra ferramenta que ela indica, de forma menos clara que o relatório, é o processo de avaliação sistemática de impactos e riscos à privacidade,[5] que nada mais é do que uma avaliação de impacto. Esta 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.

Considerando que o relatório e a avaliação de impacto se apresentam como ferramentas fundamentais para a realização de processos de conformidade com legislações de proteção de dados, neste artigo procuramos apresentar ao leitor o que é o relatório de impacto à proteção de dados, a partir de uma análise crítica e interpretativa da sua definição na LGPD.

## 2 Relatório de impacto à proteção de dados na LGPD

### 2.1. Origem: de onde vieram os relatórios?

Antes da sanção da LGPD já existiam no Brasil mais de 40 normas setoriais de proteção de dados, como o Código de Defesa do Consumidor, Código Civil, Marco Civil da Internet, entre outros, no entanto, apesar da existência desse conjunto expressivo, é a primeira vez que um instrumento como o relatório de impacto à proteção de dados tem previsão no ordenamento jurídico brasileiro. E apesar de os relatórios de impacto serem novos em termos de instrumento previsto na legislação brasileira, a bem da verdade é que eles já eram uma ferramenta existente há pelo menos duas décadas na legislação de proteção de dados na União Europeia (UE), a qual foi uma das fontes de inspiração para a elaboração da LGPD.

**4.** BRASIL. Lei nº 13.709/2018. Art. 5º, inciso XVII.

**5.** BRASIL. Lei nº 13.709/2018. Art. 50, § 2º, alínea *d*.

No caso, os primeiros *Privacy Impact Asssessment* (PIA)[6] foram previstos na Diretiva nº 95/46/EC (Diretiva)[7] e estavam relacionados a prevenção e mitigação de riscos envolvendo possíveis violações aos direitos dos titulares. Mas um fato curioso é que antes mesmo de serem indicados na Diretiva, eles foram inspirados através da ideia da legislação ambiental na UE, que adotava, em um primeiro momento, uma perspectiva de risco e, em um segundo momento, a necessidade de apreciação dos riscos em avaliações de impacto que tinham como objetivo a prevenção desses riscos para o meio ambiente e para os seres humanos.

Em outras palavras, a base regulatória europeia do relatório de impacto está intimamente associada a uma perspectiva de risco, ou seja, identificar, mitigar e, principalmente, prevenir riscos ao meio ambiente e a indivíduos que possam ser afetados. Percebe-se que o objetivo do relatório, de acordo com a perspectiva ambiental, não é corrigir riscos ou os danos causados por esses, mas sim prevenir a existência deles, uma vez que os danos ambientais são em sua maioria irreparáveis. Portanto, a ideia fundamental por trás do relatório é um diagnóstico de prevenção e não de reparação.

Por mais que a fonte de inspiração para a elaboração do PIA na Diretiva tivesse como objetivo a prevenção, fato é que no texto da Diretiva o PIA foi incorporado como uma mera recomendação de elaboração de relatório focado em avaliação de riscos, e sem força vinculante como instrumento jurídico na legislação europeia e, por esse motivo, naquela época eram poucas as empresas que conduziam esse instrumento dentro de suas organizações. Anos mais tarde, em 2016, com a reforma e atualização da Diretiva, os PIA ganharam um novo recorte e formatação na GDPR, legislação que substituiu a Diretiva nº 95/46/EC na UE, e se tornaram os *Data Protection Impact Assessment* (DPIA).[8] Com uma indicação mais precisa das situações em que os relatórios seriam mandatórios – processamento de dados que pudesse gerar altos riscos aos direitos e liberdades das pessoas naturais[9] –, a GDPR conseguiu o que a Diretiva não fez, que foi tornar os relatórios de impacto destaque no cenário regulatório de proteção de dados no mundo (GOMES, 2019).

A base regulatória europeia do relatório de impacto está associada a uma perspectiva de risco.

O DPIA, que serviu de fonte inspiradora para a criação da ferramenta do relatório de impacto na LGPD, tem como objetivo a identificação, mitigação e prevenção de riscos e altos riscos aos titulares de dados. Este documento é o resultado de um processo de avaliação de impacto, e deve ser visto não apenas como uma documentação do controlador[10] gerada após um processo de conformidade, mas sim como um instrumento de apoio nas atividades de tratamento de uma organização para que ela possa fazer sua governança de dados e demonstrar conformidade com as obrigações legais previstas.

Dessa forma, podemos concluir que o relatório de impacto à proteção de dados na LGPD vem de

**6.** UNIÃO EUROPEIA. Diretiva nº 95/46/EC. Consideranda nº 46: "whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected".

**7.** A Diretiva era a legislação geral de proteção de dados da UE e que foi substituída pela General Data Protection Regulation (GDPR) em 2016, quando ela foi revogada.

**8.** UNIÃO EUROPEIA. Regulamento nº 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Art. 35.

**9.** UNIÃO EUROPEIA. Regulamento nº 2016/679 do Parlamento Europeu e do Conselho, de 27 abril de 2016. *General Data Protection Regulation*. Consideranda nº 84.

**10.** BRASIL. Lei nº 13.709/2018. Art. 5º, inciso VI: "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

uma ideia de organização sistemática das operações de tratamento de dados, a fim de viabilizar a visualização de processos e procedimentos internos, bem como o tratamento de dados existentes, para que seja possível através dele realizar a prevenção de riscos e a mitigação desses, caso eles já sejam existentes.

Assim, compreender o seu contexto e as funções que ele pode desempenhar numa governança de dados interna e ao mesmo tempo com um papel de atuação nacional é essencial para a construção de um modelo de uso de dados mais refinado e maduro no Brasil (GOMES, 2019).

## 2.2. Afinal, o que é o relatório de impacto?

De acordo com o art. 5º, inciso XVII, da LGPD, o relatório de impacto à proteção de dados é uma 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 desses riscos.

Para uma análise mais detida em relação a essa definição trazida pela lei, vamos segmentá-la em três partes: (i) documentação do controlador; (ii) descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais; e (iii) medidas, salvaguardas e mecanismos de mitigação desses riscos.

Quando a LGPD dispõe que o relatório de impacto é uma documentação, ela instrumentaliza a forma como ele deve existir e ser apresentado perante a ANPD, ou seja, como um documento formal que atende aos critérios descritos na continuação da definição do termo. Vale ressaltar que a ANPD poderá dispor como esse documento deve ser e o que ele deve conter. A título exemplificativo, várias ANPDs em outros países, como o Information Comissioner Officer (ICO) do Reino Unido, disponibilizam informações, modelos e exemplos de como deve ser a estrutura de um relatório de impacto.

No caso do ICO, esta autoridade indica que os DPIA devem:[11] (i) descrever a natureza, escopo, contexto e finalidades do processamento; (ii) avaliar a necessidade, proporcionalidade e medidas de conformidade; (iii) identificar e avaliar riscos para indivíduos; e (iv) identificar quaisquer medidas adicionais para mitigar esses riscos (tradução livre).

Já no caso da CNIL, ela fornece modelos[12] de como deve ser a estrutura de um relatório e oferece ainda um *software* livre e gratuito[13] que auxilia na elaboração do relatório ou PIA, como a CNIL prefere nomear. Nessa hipótese, percebe-se que a ANPD pode e deve sugerir modelos e estruturas de relatório que auxiliem todos os agentes de tratamento a compreender como isso deve ser feito. Até porque vale lembrar que grande parte desses agentes são pequenas e médias empresas,[14] que não possuem condições de custear a elaboração de um relatório e todo o processo envolvido em sua realização sem que isso impacte na sua gestão de recursos internos. Portanto, a recomendação de como deve ser elaborada essa documentação é fundamental para a efetivação da LGPD.

Vale esclarecer que o texto da LGPD explicitamente associa os relatórios de impacto somente a controladores, no entanto, isso não significa que os operadores[15] também não devam ou não possam fazer um relatório. Pelo contrário, numa interpretação sistemática da lei, verifica-se que

**11.** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Acesso em: 6 set. 2019.

**12.** Disponível em: https://www.cnil.fr/en/PIA-privacy-impact-assessment-en. Acesso em: 6 set. 2019.

**13.** Disponível em: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment. Acesso em: 6 set. 2019.

**14.** SEBRAE. *Pequenos negócios em números*. Disponível em: http://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD. Acesso em: 6 set. 2019.

**15.** BRASIL. Lei nº 13.709/2018. Art. 5º, inciso VII: "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

ambos devem fazer em benefício de suas atividades de tratamento (GOMES, 2019).

Já em relação à segunda parte da análise, pergunta-se: o que seria a descrição dos processos de tratamento de dados pessoais? Neste ponto, parece que a intenção do legislador não foi que o relatório fosse uma demonstração do registro de atividades ou um inventário de dados especificamente, o qual também está previsto na LGPD[16] e no Marco Civil da Internet,[17] mas sim que contivesse uma descrição dos procedimentos que envolvem as operações de tratamento de dados, através de uma perspectiva maior de governança de dados.

## O que seria a descrição dos processos de tratamento de dados pessoais?

Ou seja, a ideia nesse ponto é fazer perguntas sobre: como funcionam internamente, na sua organização, os processos e procedimentos que são relacionados aos tratamentos e fluxo de dados interno? Afinal, a forma como o agente de tratamento trata esses dados hoje é capaz de gerar riscos?

É possível afirmar que são definidos neste escopo, a princípio, duas espécies de riscos: (i) os riscos a liberdades civis; e (ii) os riscos a direitos fundamentais. Mas antes de adentrarmos nas espécies de riscos indicadas, primeiramente, vale explicarmos de maneira sucinta o que é entendido como risco no âmbito deste estudo.

De acordo com Raphaël Gellert (2017, p. 2), a definição de risco é:

"Em poucas palavras, pode-se argumentar que o risco pode ter dois significados – um vernacular e outro mais técnico. No sentido vernacular, o risco é geralmente referido como um futuro, possível perigo, ou seja, como 'um perigo eventual que pode ser previsto apenas até certo ponto' (GODARD *et al.*, 2002, p. 12). No sentido técnico, no entanto, o risco pode ser visto como uma noção dupla. Isto é usado para tomada de decisão com base na avaliação de futuros eventos. Seus elementos constitutivos são duas operações distintas e unidas: prever eventos futuros (negativos e positivos) e tomar decisões com base nisso. Portanto, pode-se argumentar que 'qualquer decisão relacionada ao risco envolve dois e, ainda assim, elementos inseparáveis: os fatos objetivos e uma visão subjetiva sobre a conveniência do que deve se ganhar, ou perder, pela decisão" (tradução livre).

Em que pese a acepção da palavra, verifica-se que risco no contexto de proteção de dados se trata de uma questão muitas vezes subjetiva, uma vez que a partir dos riscos identificados e relatados no relatório o controlador deverá tomar uma decisão sobre de quais riscos ele deseja priorizar a mitigação e quais riscos ele deseja assumir em seu negócio, mesmo estando sujeito a uma eventual sanção prevista em lei.

Portanto, o que será avaliado durante a realização da avaliação de impacto ou, especificamente, a avaliação de risco é qual é a matriz de risco envolvida que está relacionada às liberdades civis e aos direitos fundamentais, das pessoas naturais que são os titulares de dados. A lei fala em liberdades civis no inciso que contém a definição do relatório, mas no resto da lei cita sempre como "direitos e liberdades fundamentais", o que leva à compreensão de que ela se refere mais expressamente aos seguintes aspectos: os direitos fundamentais de liberdade, intimidade e privacidade; e os direitos dos titulares indicados no capítulo III da lei.

Nesse sentido, podemos considerar como direitos fundamentais os que estão positivados no art. 5º da Constituição Federal e, como liberdades civis, a liberdade de pensamento, liberdade religiosa, liberdade de expressão e liberdade de associação. O escopo do relatório de impacto está relacionado ao

**16.** BRASIL. Lei nº 13.709/2018. Art. 37.
**17.** BRASIL. Lei nº 12.965/2014. Art. 10.

mapeamento de riscos, de forma a identificar quando existem ou podem vir a existir potenciais riscos aos titulares de dados, que, no caso, seriam riscos aos seus direitos fundamentais e liberdades civis, os quais, pela sua amplitude, podemos afirmar que estão intrinsecamente relacionados aos novos direitos dos titulares de dados, os quais estão previstos nos arts. 17 a 21 da LGPD.

Por fim, quanto à terceira parte desta análise, temos as medidas, salvaguardas e mecanismos de mitigação desses riscos. Verifica-se que aqui a lei quis indicar que o relatório de impacto tem como um dos seus objetivos o mapeamento de procedimentos de gestão de dados e de operações de tratamento de dados, para que, com isso, caso sejam identificados riscos, seja possível indicar medidas, salvaguardas e mecanismos de mitigação desses riscos. Mas o que seriam medidas, salvaguardas e mecanismos?

Como verificamos anteriormente, a natureza do relatório de impacto vem de uma base seminal que busca em primeiro lugar a prevenção. Contudo, na redação da LGPD, foi priorizada a mitigação, ou seja, a redução de danos causados por riscos e a redução dos riscos já existentes, mas que ainda não tenham gerado danos.

Como medidas, podemos compreender ações afirmativas do controlador que visem à redução dos riscos existentes ou o gerenciamento desses riscos de forma efetiva, como a decisão de um modelo de negócio de não realizar operações que envolvam dados sensíveis, por exemplo. Como salvaguardas, podemos compreender medidas preventivas que potencializam a mitigação dos riscos ou a redução dos danos causados por esses, como a contratação de um seguro específico contra incidentes de segurança, por exemplo.

E, por fim, como mecanismos podemos entender que é o conjunto de ações positivas ou negativas (fazer ou deixar de fazer) que irão contribuir para a mitigação dos riscos envolvidos em uma determinada operação de tratamento de dados, como, por exemplo, o desenho de um novo produto baseado em uma infraestrutura por desenho e concepção que garanta direitos relacionados à privacidade e à proteção de dados, a qual será conduzida e acompanhada pelo(a) encarregado(a)[18] do controlador juntamente com uma equipe de especialistas, os quais desenvolverão e analisarão aquele novo produto, para que ele possa estar alinhado com a governança de dados da empresa.

Percebe-se com essas considerações que a definição do relatório de impacto prevista na LGPD não tem como objetivo indicar todos os pormenores que envolvem a elaboração de um relatório, uma vez que parte elucidativa de como utilizar essa ferramenta está a cargo da ANPD. Por essa razão, é essencial que esse seja um tema cada vez mais debatido, a fim de ser compreendido o efetivo papel do relatório de impacto.

### 2.3. Qual é o papel do relatório de impacto?

Os relatórios de impacto, em uma perspectiva de adequação à LGPD e sem a intenção de exaurir a análise desse tema, são, em síntese, o resultado de uma avaliação de impacto que tem como objetivo avaliar, mapear, planejar, implementar e monitorar todo o processo de conformidade com as leis gerais e setoriais de proteção de dados. Numa analogia simples é o diagnóstico das atividades de tratamento de dados de uma organização.

É comum a associação do relatório de impacto como resultado ou produto de um processo de conformidade em relação à LGPD, ou seja, como uma documentação que indica todo o mapeamento realizado, com indicação dos riscos identificados e as formas que o controlador pretende adotar para a mitigação desses riscos. Tudo isso como forma de demonstrar "conformidade" com as obrigações da lei e, mais ainda, como umas das formas de

**18.** BRASIL. Lei nº 13.709/2018. Art. 5º, inciso VIII: "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

conseguir demonstrar responsabilidade e prestação de contas[19] (*accountability*) perante a ANPD.

Contudo, é importante esclarecer que o relatório de impacto não é uma ferramenta que visa atender apenas aos processos de conformidade com a LGPD. A ideia do relatório de impacto é refletir uma avaliação de impacto, cuja base regulatória é a identificação de riscos, que pode ser realizada para propósitos diferentes, como: avaliar o impacto de incidentes de segurança; avaliar o impacto de novas tecnologias; avaliar o impacto de novos produtos que podem gerar riscos aos direitos dos titulares de dados, etc.

> A ideia do relatório de impacto é refletir uma avaliação de impacto.

Cada uma dessas avaliações de impacto resultará em um relatório de impacto à proteção de dados diferente. Portanto, quando realizamos um processo de conformidade com uma legislação, e aqui nosso exemplo é a LGPD, estamos, na verdade, nos referindo a uma avaliação de impacto regulatória, a qual irá olhar para todas as obrigações constantes na lei, verificar o nível de conformidade existente de uma organização em relação a essas obrigações e quais são os riscos envolvidos no cumprimento ou não de cada uma delas, tendo como fundamento basilar a prevenção.

Este é o primeiro passo: entender que, nesse momento que precede a entrada em vigor de uma nova legislação, é necessário fazer uma avaliação de impacto regulatória, mas que isso não impede que outras avaliações de impacto e outros relatórios de impacto, que possuam escopo e objetivos diferentes, sejam realizados dentro de uma mesma organização. Nesse sentido, em paralelo ao processo de conformidade em si, pode e é recomendado que sejam feitas avaliações de impacto no desenvolvimento de novos produtos, por exemplo. A título exemplificativo, se um novo produto que uma empresa pretende lançar envolve testes de dados genéticos em pessoas naturais, é essencial que seja a princípio avaliado qual será o impacto desse novo produto na empresa e nos titulares de dados. Por exemplo, é necessário verificar como será feito o teste para preservar e atender aos direitos dos titulares, qual é o nível de risco associado a possíveis incidentes de segurança, se questões éticas e direitos fundamentais do ser humano serão atendidos, etc.

Ou seja, o papel do relatório de impacto é ser uma ferramenta de governança de dados a ser internalizada no cotidiano da organização, não apenas um documento para ser utilizado durante um processo de adequação regulatória. Isso para que todos os processos que envolvam tratamento de dados, atuais e novos, possam garantir o atendimento e a preservação dos direitos dos titulares de dados.

Em tese isso não está longe da realidade atual. No caso, quando é solicitado, por exemplo, um parecer sobre um produto que será lançado ou sobre um modelo de negócio, serão avaliados os riscos associados, potenciais questões a serem resolvidas antes, ou potenciais riscos jurídicos relacionados ao tipo do produto em si, ou ao público a que ele é direcionado, etc. O que vai diferenciar o clássico parecer jurídico do relatório de impacto é a forma como este último é instrumentalizado, qual é a metodologia que ele segue para fazer essa análise e quais são os riscos não apenas jurídicos, mas também éticos que a tecnologia embutida no produto pode causar aos seres humanos.

Quando olhamos para a ferramenta do relatório de impacto e a avaliação que o precede, precisamos usá-la de acordo com os desafios existentes hoje, em nossa sociedade contemporânea, até porque as operações atuais de tratamento de dados

**19.** BRASIL. Lei nº 13.709/2018. Art. 6º, inciso X.

podem ser muitas vezes massivas e invasivas, e no futuro, devido ao avanço tecnológico, podem se tornar ainda mais. Nesse sentido, é fundamental que orientações sobre quais operações de tratamento de dados podem acarretar riscos aos titulares de dados sejam exemplificadas pela ANPD desde já, bem como que essas recomendações sejam elaboradas de forma didática e acessível, a fim de cumprir o seu papel, que é de orientar e não de burocratizar a elaboração dos relatórios de impacto à proteção de dados.

Como vimos, a análise do risco e a classificação deste pode ser muitas vezes subjetiva, portanto, é relevante que sejam traçadas orientações a servir de guia para os agentes de tratamento entenderem como mensurar esses riscos, através do desenvolvimento de uma matriz de risco baseada em uma metodologia de avaliação, durante a avaliação de impacto e, posterior, indicação no relatório de impacto.

Exemplo semelhante foi feito pelo antigo Article 29 Working Party Group (WP29), atual European Data Protection Board (EDPB),[20] o qual em 2017 traçou diretrizes e esclarecimentos sobre o tema. Com orientações mais claras e precisas, o "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" (ARTICLE 29, 2016) solidificou o cenário das hipóteses em que o DPIA seria mandatório e qual seria a estrutura básica que ele deveria conter.

As hipóteses indicadas nas recomendações trazem luz para o que seria considerado um tratamento suscetível de resultar num elevado risco.[21] e [22] Para tanto, foram elencadas situações como: (i) tratamento de dados que envolva decisões automatizadas relacionadas a perfilamento; (ii) operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo art. 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o art. 10; ou (iii) controle sistemático de zonas acessíveis ao público em grande escala (*ibidem*, p. 9-10).

Em consonância com as orientações do WP29, o Conselho da Europa também reforçou a recomendação da elaboração de relatórios durante a revisão do texto da Convenção nº 108 em 2018.[23] Nela também foram recomendadas a análise do impacto do tratamento dos dados sobre os direitos e liberdades fundamentais dos titulares, para controladores e, quando for o caso, operadores.

Em outras palavras, o relatório precisa ser um reflexo do nosso tempo e dos desafios atuais que enfrentamos no contexto brasileiro, e a orientação e recomendação a serem feitas pela ANPD devem ser relacionadas e direcionadas a essa realidade, a fim de que ele possa ser uma fotografia precisa dos problemas enfrentados pelos agentes de tratamento no Brasil em diversas operações de tratamento de dados.

Por mais que o relatório por analogia possa ser encarado como uma "fotografia", a qual deve guiar e orientar os agentes de tratamento a sempre melhorarem suas operações envolvendo dados, e ajudá-los nas tomadas de decisão, fato é que ele não deve ser encarado como um documento frio,

**20.** Grupo de trabalho formado pelas Autoridades de Proteção de dados na UE (*Data Protection Authorities "DPA"* ou *Supervision Authorities*) e que atuou até 2016, quando o EDPB assumiu essa função.

**21.** Para fins de facilidade de interpretação, iremos considerar as terminologias traduzidas para o português de Portugal no documento do WP29.

**22.** 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, revistas e adotadas pela última ➔ vez em 4 de outubro de 2017. "O RGPD não exige a realização de uma AIPD para todas as operações de tratamento que possam implicar riscos para os direitos e as liberdades das pessoas singulares. A realização de uma AIPD é obrigatória somente quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (art. 35, nº 1, ilustrado pelo art. 35, nº 3, e complementado pelo art. 35, nº 4). É particularmente importante quando se introduz uma nova tecnologia de tratamento de dados11" (ARTICLE 29, 2016, p. 9).

**23.** Council of Europe. Convention 108+: the modernised version of a landmark instrument. Disponível em: https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108. Acesso em: 6 set. 2019.

estático, engavetado ou meramente guardado nas pastas do *drive* dessas organizações.

Todos os dias, trilhões de dados (ou mais) são tratados em nossa sociedade. A proposta da UE com o relatório de impacto, que foi posteriormente tropicalizada no Brasil por meio da LGPD, não foi gerar um calhamaço de documentos para comprovar que está tudo certo dentro das organizações, mas sim e, essencialmente, figurar como uma ferramenta dinâmica, capaz de auxiliar na governança de dados e na mitigação dos riscos associados às operações de tratamento de dados. Guardá-lo em caixinhas é submetê-lo ao esquecimento, esvaziando o seu propósito.

## 3 Conclusão

O relatório de impacto à proteção de dados não deve ser enxergado na LGPD como uma ferramenta burocrática, mas sim como uma documentação que reflete um processo de aprendizado por agentes de tratamento, que é o de realizar a governança de dados dentro de casa.

Nesse sentido é importante finalizar a leitura entendendo o seguinte: (i) relatórios de impacto em proteção de dados são novos no ordenamento brasileiro, mas bebem de uma fonte mais antiga, no caso a da regulação de proteção de dados da UE; (ii) relatórios de impacto não servem apenas para processo de conformidade ou adequação a uma lei; (iii) relatórios de impacto não são apenas um critério para demonstração de *accountability*; (iv) a ANPD precisa elaborar modelos e orientações sobre como fazer um relatório de impacto e tornar essas recomendações acessíveis em linguagem e custo; (v) a ANPD precisa emitir orientações sobre o que é considerado risco ou um possível alto risco em operações de tratamento de dados; (vi) o papel do relatório é ser uma ferramenta efetiva de governança de dados, que reflita uma análise dos tratamentos de dados realizados e ajude na tomada de decisões futuras.

Na prática, o que vai ocorrer, nesse momento de adequação da LGPD, é a realização de uma grande avaliação, por parte dos agentes de tratamento, e diga-se: avaliação de impacto regulatória, com o propósito de ser buscada uma conformidade regulatória. Aqui pedimos licença para afirmar e fazer "futurologia" para dizer que boa parte do mercado (independentemente do setor) buscará ter um relatório de impacto à proteção de dados em sua gaveta, ou seu *drive*, caso a ANPD, ou mesmo outros, venham a fazer qualquer tipo de solicitação sobre a apresentação do documento.

Contudo, guardá-lo e arquivá-lo está longe de ser o propósito da elaboração de um relatório de impacto. É necessário compreender que este é um documento "vivo", reflexo cotidiano das operações de tratamento e da tomada de decisão dos controladores. E, por esse motivo, ele precisa ser atualizado constantemente, a fim de cumprir o seu papel de ferramenta que auxilia na construção da governança de dados de uma organização e, consequentemente, contribui para o desenvolvimento de um ecossistema saudável de uso de dados no Brasil. ■

## Bibliografia


ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Statement on the role of a risk-based approach in data protection legal frameworks. Adopted on 30 May 2014, WP 218. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

BENNETT, Colin J.; RAAB, Charles D. *The Governance of Privacy*: policy instruments in global perspective. 2nd and updated ed. Cambridge, Mass: MIT Press, 2006.

BINNS, Reuben. Data protection impact assessments: a meta-regulatory approach. *International Data Privacy Law*, v. 7, n. 1, 2017.

COUNCIL OF EUROPE. *Convention 108+*: the modernised version of a landmark instrument. Disponível em: https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108.

COUNCIL OF EUROPE. *Handbook on Data Protection Law*. Disponível em: https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf.

GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice* (2017). Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917302698.

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

QUELLE, Claudia. *The Data Protection Impact Assessment, or*: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing (November 25, 2015). Disponível em: https://ssrn.com/abstract=2695398.

QUELLE, Claudia. *The 'Risk Revolution' in EU Data Protection Law*: We Can't Have Our Cake and Eat It, Too. Rochester, NY: Social Science Research Network, 2017. Disponível em: https://ssrn.com/abstract=3000382.