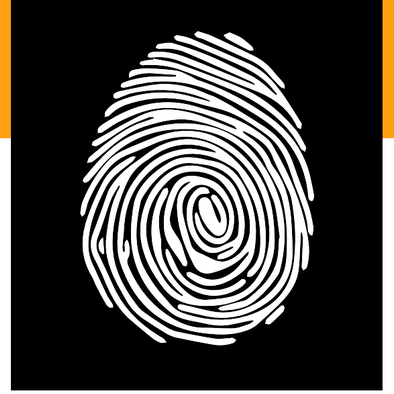


Relatório de Impacto à Proteção de Dados Pessoais

Aspectos práticos relevantes à luz da LGPD

Índice

Estrutura do documento

Conteúdo elaborado por: Caio César Carvalho Lima; Luanna Rodrigues Peporini; Marcilio Braz Júnior; Maria Fernanda Hosken Perongini; Núria Debaza Bauxali; Remilina Yun (Remi); Raphael Dutra da Costa Campos.

Organizadora: Remilina Yun

Imagens: Pixabay / Canva

Apresentação

LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018)

No dia 14 de agosto de 2018 foi sancionada no Brasil a Lei Geral de Proteção de Dados (LGPD), inaugurando noviço cenário regulatório em nosso país ao instituir um microssistema regulatório acerca do tema, tendo sido a Lei bastante influenciada pelo Regulamento Geral de Proteção de Dados Europeu (do inglês GDPR – *General Data Protection Regulation*).

Com isso, a partir da eficácia plena da norma, prevista para fevereiro de 2020, será superado o atual regime setorial de abordagem do tema (com esparsas previsões em diversas leis, tais como o Código Civil, Código de Defesa do Consumidor, Marco Civil da Internet, Lei do Cadastro Positivo, Lei de Acesso à Informação, entre outros), passando-se a endereçar as questões relacionadas ao tratamento (coleta, uso, armazenamento, compartilhamento, exclusão, entre outros) de dados pessoais (qualquer informação que identifique ou torne identificável uma pessoa física) por meio de uma lei geral.

Várias questões passam a ser fundamentais para que todos os agentes envolvidos no tratamento de dados (quer como controlador ou operador) fiquem *compliant* com referida norma, mitigando as eventuais sanções a que podem ficar expostos, em decorrência de incidentes de segurança.

Entre outros, é relevante bem entender o que diz respeito ao Relatório de Impacto à Proteção aos Dados (RIPD), o qual mereceu conceito específico na LGPD, conforme se observa do inciso XVII do artigo 5º, que faz alusão a esse relatório como sendo a "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".

Em linhas gerais, pois, esse RIPD deve contemplar o registro de todas as operações com dados pessoais, especialmente quando a base legal para o tratamento for o legítimo interesse (artigo 37), ou quando dados pessoais sensíveis forem objeto de tratamento (artigo 38), identificando os principais riscos relacionados às atividades, bem como o que será realizado para mitigá-los.

Assim, apesar de inúmeras situações concretas de tratamento de dados estarem abarcadas pelo conceito acima, pouco foi especificamente disciplinado na nossa legislação e na doutrina especializada, restando inúmeras dúvidas acerca desse RIPD, considerando a aplicação prática. Em decorrência disso, dentro de grupo de estudos que foi criado por Dirceu Santa Rosa e Remilina Yun (Remi), resolvemos, juntamente com Marcílio Braz Júnior, Maria Fernanda Hosken, Luanna Rodrigues Peporini, Núria Baxauli, José Vitor e Raphael Dutra, endereçar os principais aspectos que devem ser considerados para a elaboração de um RIPD, o que passaremos a endereçar em uma série de artigos, a serem publicados nesta Revista, ao longo dos próximos meses.

A ideia é que inicialmente seja abordado como o GDPR influenciou a nossa LGPD, no que concerne à elaboração do RIPD, indicando também em quais situações se entende que há obrigatoriedade de produzir o Relatório,

abordando também as exceções trazidas nas legislações, mencionando os casos em que se recomenda elaborar o Relatório, ainda que não seja mandatório.

Em seguida, serão traçados aspectos práticos do RIPD, endereçando o conteúdo mínimo do Relatório, as principais etapas de elaboração (com detalhamento das fases principais) e endereçando o tempo de guarda dos relatórios, bem como sua periodicidade de atualização.

Por fim, serão abordadas questões específicas de governança, posicionado o RIPD dentro das melhores práticas sobre o assunto, adentrando também o tema de incidentes de segurança da informação e identificando como o Relatório pode colaborar para mitigar essas questões.

Introdução

Avaliação de Impacto sobre a proteção de dados pessoais

Maria Fernanda Hosken Perongini

Introdução

Avaliação de Impacto sobre Proteção de Dados

Avaliação de Impacto sobre a Proteção de Dados (ou DPIA, derivado do acrônimo em inglês *Data Privacy Impact Assessment*) é o nome dado ao processo que analisa e documenta o impacto futuro que o processamento dos dados pessoais terá sobre seus titulares. Por “impacto na privacidade" entende-se as consequências - possivelmente indesejadas - que o processamento de dados pode impor aos indivíduos ou à sociedade.

A ideia de avaliações de impacto na privacidade surgiu nos anos 1970, mas seu conceito amadureceu durante o período 1995-2005, como uma reação pública tardia contra as ações cada vez mais invasivas de privacidade por parte de governos e corporações durante a segunda metade do século XX [1]. A adoção de DPIAs pelas organizações se consolidou ao longo dos anos, sendo incorporada às estruturas de avaliação de risco como resultado dos danos reputacionais decorrentes de violações à privacidade, então já considerada uma variável estratégica [1].

Embora o termo DPIA tenha se tornado popular, não há um método sistemático para realiza-lo, havendo inúmeras orientações e listas de verificação publicadas por autoridades nacionais e organizações especializadas. Entretanto, algumas características distinguem tais relatórios de outros tipos de atividades pelas seguintes características:

❑ Possui natureza antecipatória (ou seja, um DPIA é distinto de uma auditoria de privacidade);
❑ Tem amplo escopo (em relação às dimensões de privacidade, perspectivas externas e expectativas dos titulares e governos);
❑ É orientado para analisar o surgimento de problemas e elaboração de soluções;
❑ Enfatiza o processo de avaliação, incluindo troca de informações, aprendizado organizacional e adaptação de design;
❑ Exige engajamento e envolvimento intelectual da alta direção (diretores e gerentes seniores).

Nos próximos artigos, serão analisados os casos de obrigatoriedade (e exceções legais) no tocante à elaboração de DPIAs, à luz da GDPR e da LGPD. Passa-se, então, ao exame dos aspectos práticos do processo de elaboração do relatório, bem como suas etapas de desenvolvimento, tempo de guarda das informações levantadas e considerações a respeito da periodicidade da atualização do DPIA.

Por fim, a elaboração de DPIAs é analisada à luz dos princípios de governança corporativa, tendo sempre em vista a conformidade exigida pela nova lei brasileira.

***DATA PRIVACY IMPACT ASSESSMENT (DPIA)* ou**

Relatório de Impacto à Proteção de Dados

Luanna Rodrigues Peporini e Raphael Dutra da C. Campos

Relatório de Impacto à Proteção de Dados

DA SUA OBRIGATORIEDADE NO LGPD E GDPR

"Tal avaliação deve ser feita sempre antes do início do tratamento dos dados".

O GDPR, em sua Seção 3, artigo 35, trata da realização de uma avaliação de impacto sobre a proteção de dados, sempre que o tratamento dos dados pessoais levar a um risco elevado para os direitos e liberdades dos titulares dos dados, considerando as tecnologias usadas, natureza, âmbito, contexto e finalidades do tratamento dos dados. Tal avaliação deve ser feita sempre antes do início do tratamento dos dados.

O item 3 do artigo 35 acima mencionado traz as hipóteses nas quais a realização da avaliação de impacto sobre a proteção de dados é obrigatória, sendo elas, em suma:

(a) avaliações sistemáticas e completas de pessoas naturais, incluindo a definição de perfis, mais conhecida como *profiling*, e sobre as quais decisões que produzam efeitos jurídicos ou que afetem o titular dos dados são tomadas;
(b) realização de operações de tratamento de dados sensíveis ou dados relacionados com condenações penais e infrações, em grande escala; ou

c) monitoramento sistemático de áreas acessíveis ao público em geral, em grande escala.

Vale ressaltar que as autoridades de controle de cada Estado-Membro, nos termos do artigo 35, item 4, devem elaborar e tornar públicas suas listas dos tipos de operações que entendem estarem sujeitas à realização da avaliação de impacto. Ainda, nos termos do item 5, do artigo 35, as autoridades também podem elaborar listas de atividades que consideram prescindir da avaliação de impacto.

Diferentemente do GDPR, que contém uma Seção específica para tratar da elaboração da avaliação de impacto, a LGPD traz disposições esparsas sobre a realização da avaliação de impacto, chamada na LGPD de relatório de impacto à proteção de dados pessoais.

A elaboração do relatório de impacto é citada, pela primeira vez, no parágrafo 3º do artigo 4º, inciso III, enquanto isso, o inciso III do artigo 4º dispõe sobre hipóteses de não aplicação da LGPD, mais especificamente, quando o tratamento dos dados pessoais for realizado para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais.

O parágrafo 3º do artigo 4º faz referência ao citado inciso III, prevendo que a autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

A previsão acima parece contraditória, na medida em que, se afastada a aplicação da LGPD, nos casos previstos no inciso III do artigo 4º, não haveria que se falar na elaboração de relatórios de impacto, exceto se a elaboração do relatório de impacto servir exatamente para determinar se o tratamento dos dados pessoais realmente se enquadra nas hipóteses previstas no inciso III.

A elaboração do relatório de impacto à proteção de dados pessoais é citada também no parágrafo 3º do artigo 10 da LGPD, que trata de exemplos nos quais é permitido o

tratamento de dados com base no legítimo interesse do controlador. O mencionado parágrafo 3º prevê que a autoridade nacional poderá solicitar ao controlador a elaboração de relatório de impacto quando o tratamento dos dados tiver como base legal o legítimo interesse.

O Capítulo IV da LGPD, que dispõe sobre o tratamento de dados pessoais pelo Poder Público também contém uma previsão sobre a elaboração do relatório de impacto. O artigo 32 da LGPD, último artigo do Capítulo IV, prevê que a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais.

O artigo 38 da LGPD é o último a tratar da elaboração do relatório de impacto à proteção de dados pessoais, prevendo que 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.

Assim, diferentemente do GDPR que traz hipóteses nas quais a realização da avaliação de impacto é obrigatória, sem prejuízo de listas a serem emitidas pelas autoridades do Estados-Membros, parece-nos que a elaboração do relatório de impacto prevista na LGPD depende sempre de solicitação da autoridade nacional e de regulamento a ser emitido. Considerando que os artigos que previam a criação da autoridade nacional foram vetados, enquanto não criada a autoridade, resta prejudicada a interpretação sobre a necessidade de elaboração dos relatórios de impacto.

Considerando que a LGPD foi inspirada fortemente pelo GDPR e contém princípios muito parecidos, enquanto não houver a criação da autoridade nacional e, portanto, a publicação de regulamentos ou orientações sobre a elaboração do relatório de impacto, sugerimos que os controladores, sujeitos à LGPD, sigam as hipóteses de obrigatoriedade previstas no GPDR.

Relatório de Impacto à Proteção de Dados

DA SUA EXCEÇÃO

"Em outras palavras, o relatório de impacto à proteção de dados pessoais é um processo que visa estabelecer mecanismos de mitigação de risco e demonstrar a conformidade com a regulamentação, através de um documento."

Como se pode observar, o Relatório de Impacto à Proteção de Dados Pessoais é um documento que tem sua origem em um processo dinâmico, isto é, um processo que precisa sempre estar sendo monitorado e revisitado, de forma que haja uma fotografia verossímil do status da conformidade regulatória e, também, da mitigação dos riscos identificados e postos aos titulares. Em outras palavras, o relatório de impacto à proteção de dados pessoais é um processo que visa estabelecer mecanismos de mitigação de risco e demonstrar a conformidade com a regulamentação, através de um documento.

Portanto, é evidente que existem situações em que, embora não mandatório, é desejável a produção de um relatório de impacto à proteção de dados pessoais, pois, o conceito de “risco” é inerente à análise contextual específica, podendo ser entendido, de forma geral, como um cenário que descreve um acontecimento e as respectivas consequências deste fato, de acordo com seu grau de probabilidade e gravidade.

Assim, as melhores práticas internacionais de proteção de dados pessoais nos ensinam que é particularmente importante desenvolver um processo que vise estabelecer mecanismos de mitigação de riscos suscetíveis em gerar impactos às liberdades civis e aos direitos fundamentais, quando se introduz uma nova tecnologia de tratamento de dados pessoais.

Ademais, ainda de acordo com as melhores práticas internacionais de proteção de dados pessoais, existem nove critérios que devem ser observados para entender quando uma atividade de tratamento é suscetível em gerar impactos às liberdades civis e aos direitos fundamentais, são eles:

(i) Avaliação ou "score" (pontuação). Um exemplo bem claro em relação a este critério ocorre quando uma instituição financeira faça uma análise seletiva de seus clientes a partir de uma base de dados que tenham como referência um "*credit score*", ou seja, que se referenciem ao crédito bancário.

(ii) Decisões automatizadas. O tratamento automatizado pode significar um tratamento que, por vezes, poderá ser considerado discriminatório, dessa forma, os titulares dos dados pessoais têm como direito o "*right to explain*", estabelecido pelo artigo 20 da LGPD, que assegura que o titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

(iii) Monitoramento ou Controle sistemático. Quando há algum tipo de controle sistemático e monitoramento de titulares de dados, isso deve ser um critério levado em consideração quando da produção de um Relatório de Impacto à Proteção de Dados Pessoais, pois, os dados pessoais podem ser recolhidos em circunstâncias em que os titulares dos dados podem não estar cientes de quem está a recolher os seus dados e da forma como esses dados serão utilizados.

(iv) Dados Pessoais Sensíveis. Dados pessoais sensíveis demandam maior rigor na observância das regras para as

para as atividades de tratamento, pois, como o próprio nome já diz, são categorias de dados pessoais especiais, logo, os riscos que derivam desse tipo de tratamento são maiores e, portanto, podem gerar maior impacto às liberdades civis e aos direitos fundamentais.

(v) Tratamento de Dados em larga escala. Para se entender o conceito de larga escala, devemos levar em consideração o número de titulares envolvidos, o volume de dados tratados, a duração da atividade de tratamento e a dimensão geográfica em que a atividade de tratamento ocorre.

(vi) Combinação de dados com origens distintas. A combinação de dados com base em duas ou mais operações de tratamento distintas pode exceder a finalidade e também da legitimidade do tratamento originário que fora estabelecido e, portanto, acabam por gerar um risco maior.

(vii) Dados relativos à titulares vulneráveis. Esse critério é devido ao 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.

(viii) Soluções inovadoras ou aplicação de novas soluções tecnológicas. A utilização de uma nova tecnologia pode desencadear a necessidade de realização de um Relatório de Impacto à Proteção de Dados Pessoais, pois novas tecnologias demandam novas formas de coleta, armazenamento e utilização dos dados.

(ix) Quando a atividade de tratamento impede o titular de exercer um direito ou utilizar um serviço. Incluem-se aqui as atividades de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato. Um exemplo claro deste critério é quando um banco faz uma análise dos seus clientes a partir de um "*credit score*" para decidir se lhes concede ou não um empréstimo.

Podemos concluir que a exigência de um DPIA é proporcional à observância dos critérios acima. Quantos mais critérios forem satisfeitos, maior é a probabilidade da necessidade de se elaborar um processo que vise mitigar riscos às liberdades civis e aos direitos fundamentais.

Por outro lado, uma atividade de tratamento de dados pessoais pode corresponder aos casos acima e, mesmo assim, o responsável pelo tratamento considerar ser uma situação que não demanda risco algum e, se este for o caso, o responsável deverá justificar e documentar as razões que o levaram a não realizar o relatório e registrar a opinião do encarregado da proteção de dados.

Conteúdo de un DPIA

Núria Debaza Baxauli

Conteúdo de um DPIA

O que deve conter um processo/relatório DPIA?

De acordo com o GDPR o DPIA deve ser realizado para avaliar, em particular, a origem, natureza, particularidade e severidade dos riscos do tratamento de dados pessoais aos direitos e liberdades dos indivíduos [2]. Neste sentido, o GDPR prevê que o documento deve incluir as medidas, salvaguardas e mecanismos adotados para mitigar o risco, assegurando a proteção dos dados pessoais e demonstrando *compliance* com o regulamento [3].

O GDPR traz ainda uma listagem do conteúdo mínimo de um DPIA, em seu artigo 35:

“7. A Avaliação inclui, pelo menos:
a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

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

Adicionalmente, quando for apropriado, é possível incluir no documento a opinião dos titulares de dados ou dos seus representantes sobre o tratamento dos dados.

Também é importante ressaltar o papel do operador dos dados neste processo, sendo que o GDPR menciona o seu dever de auxiliar o controlador quando for necessário e quando solicitado durante o processo do DPIA.

Diante deste panorama trazido pelo GDPR, passamos ao texto da LGPD, considerando que além de o DPIA ser uma obrigação legal das normas de proteção de dados para alguns casos específicos, este procedimento é recomendável para a análise de qualquer projeto e de toda empresa, de forma que o conteúdo sugerido no GDPR e LGPD podem ser usados como guia para sua realização.

A LGPD conceitua o relatório de impacto à proteção de dados pessoais como a "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".

Em seu artigo 38, a LGPD determina que a autoridade nacional poderá solicitar um DPIA sobre suas operações de tratamento de dados, incluindo dados sensíveis, mas devem ser resguardados os segredos comercial e

industrial, de forma que certos detalhes que sejam sensíveis do ponto de vista concorrencial da empresa não devem ser incluídos.

Diante do exposto sobre os textos legais da LGPD e GDPR, entendemos que após a verificação da necessidade de realização de um DPIA, será necessário delimitar o que é preciso incluir neste documento em observância ao princípio da responsabilização e prestação de contas.

Neste sentido, é possível obter maiores detalhes sobre o que é esperado de um DPIA nos guias emitidos pelas autoridades de proteção de dados da União Europeia e pelo *Information Comissioners Office* – ICO.

De forma geral, os guias mencionam as seguintes fases de um DPIA:

1. Avaliação da necessidade do DPIA, diante da conveniência de desenvolver este processo.

2. Descrição do projeto e do fluxo de informações, analisando em profundidade e em detalhes as categorias dos dados, os acessos aos mesmos e as tecnologias utilizadas, bem como incluindo a base legal para o seu tratamento, analisando os princípios da necessidade e proporcionalidade.

3. Identificação dos riscos através da análise dos possíveis riscos diante das particularidades do tratamento e a avaliação da probabilidade de acontecerem e de que os danos se materializem.

4. Gestão dos riscos identificados, determinando controles e medidas a serem adotadas para eliminar, mitigar ou transferir os riscos detectados.

5. Análise de cumprimento normativo, no sentido de analisar se o produto ou serviço desenvolvido cumpre com os requerimentos legais, gerais e setoriais, em matéria de proteção de dados.

6. Elaboração de informe final contendo uma relação detalhada dos riscos identificados, recomendações e propostas para eliminá-los ou mitigá-los, tendo como destino final a direção da organização.

7. Implantação das recomendações, especificando ações a serem tomadas e alocamentos dos recursos necessários para sua execução e dos responsáveis por executá-las.

8. Revisão e monitoramento através da análise do resultado final para comprovar a efetividade do DPIA e verificação da criação de novos riscos ou detecção de outros que passaram despercebidos antes. Diante destes resultados, é possível retroalimentar e atualizar o DPIA.

Neste sentido, os itens 1 e 8 estão relacionados, uma vez que se iniciam novos DPIAs através da revisão e monitoramento.O envolvimento das áreas internas em cada uma das fases pode variar, sendo que na descrição dos processos será necessário envolver os *experts* de cada área, e em análises de risco de segurança é oportuno envolver especialistas em segurança da informação. Por fim, como já mencionamos, a consulta das partes afetadas em cada uma das fases pode ser essencial para uma correta identificação dos riscos envolvidos.

De forma prática, o conteúdo do documento envolverá respostas a questionários e documentação de processos de diversas áreas.

Etapas de elaboração do DPIA

Marcílio Braz Júnior

Etapas de elaboração do DPIA

Propósitos e fases do relatório/processo

Com a sanção da LGPD, estabeleceu-se um marco regulatório legal para abrigar toda uma gama de direitos e obrigações relativas à proteção dos dados pessoais dos indivíduos. Dentre os princípios preconizados pela lei, atentamos para a responsabilidade e prestação de contas por parte dos agentes de processamento de dados (controladores e operadores). Uma das principais ferramentas para evidenciar tanto para os cidadãos quanto ao poder público a aderência à lei consiste no Relatório de Impacto à Proteção de Dados Pessoais (doravante RIPD).

Para além de uma obrigação, quando observamos pela dimensão GRC, a depender do apetite de risco da organização, um DPIA pode ser uma excelente ferramenta a ser utilizada voluntariamente quando da utilização de tecnologias ou atividades de processamento novas. Ao encarar o DPIA dessa forma, tem-se mais uma forma de incorporar e

demonstrar ao público externo um alinhamento da cultura organizacional orientada ao Privacy by Design/Default. Em última análise, a confiança que inspira junto ao mercado como uma empresa que efetivamente tem a privacidade e a proteção dos dados pessoais de seus clientes internos e externos como prioridade, olhar DPIA como uma ferramenta auxilia ainda mais no fortalecimento da reputação da empresa. Por fim, mas não menos importante, um relatório bem conduzido, já nas fases iniciais de um desenho de processo, ajuda a identificar problemas no nascedouro, evitando assim desperdícios futuros de recursos (como dinheiro e tempo).

A definição do relatório de impacto encontra-se no artigo 5º, XVII da lei:

Art. 5º Para os fins desta Lei, considera-se:
XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Por sua vez, o artigo 38 esclarece o âmbito de aplicação do relatório, bem como, de modo extremamente sucinto, os elementos básicos que devem compô-lo:

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

Considerando que o *mens legis* no tocante a necessidade, abrangência (parcialmente) e elementos constitutivos deste relatório inspira-se no GDPR

(*General Data Protection Regulation*) da União Europeia, em nossa opinião o diploma legal pátrio findou por carecer de maiores esclarecimentos e definições quanto a ao escopo e formatação do referido relatório, em contraposição ao diploma legal europeu.

Resulta do art. 38 da LGPD que a autoridade nacional terá poderes para impor um DPIA a um controlador, caso este não o tenha realizado. Ter-se-á que analisar se essa falta de DPIA que a autoridade nacional considera essencial para o processamento de dados poderá levar a consequências por não cumprimento, por parte do controlador, desse mesmo DPIA, quer da parte da autoridade nacional quer da parte dos titulares de dados envolvidos nesse processamento de dados.

Tendo em conta a possibilidade da necessidade de elaboração do relatório de impacto em determinadas situações, como consta no artigo 10, é nossa opinião que a falta de um DPIA essencial pode ensejar razão suficiente para a aplicação de uma multa administrativa ou de processo ou processos judiciais contra o controlador, por não fundamentar o processamento de dados devidamente, conforme requer a LGPD. No entanto, exige-se da autoridade nacional uma ponderação relativamente ao DPIA, analisando, nomeadamente, o grau de risco para o titular de dados que a falta do relatório de impacto implicou. Para além disso, mesmo sem a formalização de um, poderá o controlador ter implementado medidas técnicas e organizacionais suficientes para mitigar o risco. Parece-nos que ambos os fatores referidos, entre outros (*e.g.* a falta de DPIAs ser caso único ou um entre vários, a fundamentação do controlador para não realizar o mesmo, etc.) terão de ser tidos em consideração, não sendo a multa administrativa automática pelo simples fato de o relatório de impacto não ter sido feito.

Outro ponto que nos parece importante referir é quanto a amplitude do DPIA da LGPD, quando comparado com o do GDPR. No LGPD, de forma diferente do GDPR, o risco não é tido em consideração para a realização do DPIA. Parece-nos, no entanto, inadequada a interpretação literal do artigo, que faria com que todas as atividades de tratamento tivessem de ter um DPIA associado. Ainda

relativamente a este assunto, levanta-nos questões atinentes à salvaguarda do LGPD relativamente a "*segredos comercial e industrial*" na realização de DPIAs.

O *in fine* do art. 38 nos permite interpretar como um requisito relativamente aos DPIAs solicitados pela autoridade nacional. Tal interpretação levaria à conclusão de que o DPIA solicitado pela autoridade nacional teria de ser comunicado a essa autoridade. Porque, de outro modo, sendo documentos essencialmente internos, e disponibilizados à autoridade nacional apenas em caso de uma investigação, não se alcança o objetivo da especificação relativamente à propriedade intelectual da empresa.

Ainda, tal menção parece-nos fazer entender que a mesma implica que um DPIA solicitado pela autoridade de controle terá de ser aprovado ou rejeitado por esta. Só assim se vislumbra a necessidade de respeito pelas regras da propriedade intelectual da empresa. Mas, com os responsáveis da autoridade de controle obrigados ao sigilo profissional, como se espera, não nos parece que o *in fine* do art. 38 como sendo um requisito geral para todos os DPIAs, tal poderá tornar estes elaborados com a defesa da propriedade intelectual da empresa, inauditáveis, com as empresas a escudarem-se na propriedade intelectual para não divulgar as medidas organizacionais e técnicas aplicadas.

Desta forma, muito embora com a edição da Medida Provisória nº 869 em dezembro de 2018 que criou a Autoridade Nacional de Proteção de Dados, vetada quando da sanção da Lei nº 13.709 (LGPD), espere-se uma melhor definição, dentre outras questões, às relativas a um detalhamento e orientações mais claras quanto à metodologia a ser utilizada quando da confecção do relatório bem como sugestões de *frameworks* para o documento, na ausência destas, lançamos mão das existentes para elaboração de um DPIA (*Data Protection Impact Assessment*), o equivalente ao nosso RIPD no âmbito do GDPR.

O propósito de um DPIA não é eliminar todos os riscos, mas sim minimizar a existência destes, bem como verificar

se os riscos remanescentes são justificáveis. De acordo com as orientações existentes relativas ao DPIA, este pode ser dedicado a apenas a uma única operação de processamento, bem como a um grupo de operações, desde que similares. Igualmente, também é possível que um grupo de controladores formulem conjuntamente um DPIA.

Para além de uma demanda legal, um DPIA gera uma série de benefícios que ao próprio negócio, uma vez que a sua metodologia pode implicar em revisões de processos, alinhando assim a organização a uma visão mais abrangente de *compliance*, trazendo a reboque a possibilidade de gerar ganhos financeiros e de reputação perante seus clientes. Nunca é demais lembrar que tanto a LGPD quanto o GDPR são leis voltadas para os indivíduos, não para as empresas *per se*. O que se observa, porém, é que o fato de ao se adequarem a elas, pela via natural, mudanças organizacionais ocorrem e com elas, uma otimização nos sistemas de controle e consequentemente toda uma melhoria nos aspectos organizacionais. Mais do que um custo, a conformidade em LGPD/GDPR, como é da natureza do *compliance*, é uma oportunidade de alavancar negócios. Em última análise, mais um meio de manter-se competitivo.

Antes de fazermos um resumo sobre as principais etapas que integram a elaboração de um DPIA, convém esclarecer que o mesmo, muito embora seja até mesmo por autoridades nacionais de proteção de dados europeias (como a francesa CNIL) tratado como um sinônimo de um PIA (*Privacy Impact Assessment*), tal fato não traduz perfeitamente a realidade, do ponto de vista técnico *stricto sensu*. Muito embora suas bases possam ter uma origem comum, o PIA, além de já tratar-se de um conceito bem estabelecido, em contraposição ao recém-criado DPIA através do disposto no artigo 35 do GDPR de 2016, aquele trata de uma avaliação mais abrangente com relação aos impactos em todas as dimensões da privacidade.

Por sua vez, o DPIA surge como um instrumento que tem como foco evidenciar o *compliance* quanto a práticas previstas numa legislação específica, no caso o GDPR. Em princípio as semelhanças podem induzir a pensar que se

tratam de instrumentos iguais, por abordarem aspectos que concernem a privacidade. Porém, o PIA tem uma abrangência maior, por contemplar a análise de impacto a todas as dimensões da privacidade. Por sua vez, o DPIA concentra-se num recorte limitado a atividades de processamento específicas, a saber as que envolvam e que possam vir a comprometer a proteção dos dados pessoais e violação aos direitos do indivíduo.

Feita esta importante distinção, passemos aos aspectos metodológicos para criação de um RIPD/DPIA. Muito embora não sejam exatamente iguais um DPIA e um PIA, por sua natureza e escopo, é possível lançar mão como mera referência da ISO 29134, que estabelece uma metodologia baseada em boas práticas para realização de um *Privacy Impact Assessment*. Para uma abordagem mais específica, porém, torna-se fortemente recomendado a apreciação da documentação produzida tanto pelo antigo WP29 (agora EDPB – *European Data Protection Board*), quanto da ICO e CNIL (autoridades de proteção de dados do Reino Unido e França, respectivamente) sobre DPIAs. Para entendimento prévio sobre gestão de risco, recomenda-se complementarmente a leitura da ISO 31000, que descreve os processos envolvidos (comunicação e consulta, estabelecimento de contexto, avaliação de riscos, resposta aos riscos, monitoração e reexame). É de suma importância, antes de conduzir a elaboração de um RIPD/DPIA, que sejam feitos os seguintes questionamentos:

Foi realizada uma consulta junto aos *stakeholders* internos com relação aos possíveis riscos relativos a atividade de processamento em análise, bem como os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados a proteção de dados e privacidade)?
Foram de igual forma consultados os *stakeholders* externos? Em caso afirmativo, quem, quando e com qual propósito objetivou-se a consulta?
Adicionalmente à identificação dos riscos envolvidos, ambas consultas levaram em consideração medidas de mitigação ou minimização destes riscos?

Uma vez realizado o levantamento prévio, dá-se início efetivo ao processo de elaboração do relatório.

Para efeitos de melhor compreensão, pode-se dividir um RIPD/DPIA em 3 etapas:

1. Contexto

Entendimento da organização e processos envolvidos

2. Risk Assessment

Processo de avaliação dos riscos

3. Risk Management

Gerencimento dos riscos

A partir dessa visão macro, podemos adotar uma estrutura subdividindo as etapas de um Relatório de Impacto em 6 fases, a saber:

Fase 1. Detalhamento do processamento.
Fase 2. Análise do processamento tendo em conta possíveis relações com terceiros e respectivo contato para colaboração na elaboração das fases seguintes.
Fase 3. Identificação de controles.
Fase 4. Listagem e análise de eventos e ameaças para o titular de dados quanto ao processamento dos dados pessoais.
Fase 5. Produção de relatório com sumário de análise, controles existentes e mitigação de risco, bem como propostas de medidas técnicas e organizacionais apropriadas para mitigar o risco do titular de dados, caso estas não estejam em prática.
Fase 6. Envio para aprovação ou recusa ao DPO.

A Fase 1 visa detalhar as atividades de processamento envolvidas e que são objeto do relatório. Essa descrição sistemática das operações deve observar em seu levantamento a natureza, o âmbito, o contexto e as finalidades do tratamento.

Os dados pessoais atingidos, os destinatários, as bases legais bem como o prazo de retenção devem ser igualmente detalhadas. Importante observar que essa fase implica no mapeamento/inventário de todos os dados envolvidos, bem como sua classificação e fluxos de processamento, para citar apenas alguns pontos-chave. Em condições ideais, tais processos já foram devidamente implementados.

Resta evidente, portanto, que aos considerarmos o processo de implementação de *compliance* em LGPD é no mínimo incorreto afirmar que o primeiro passo para dar início àquele seria a elaboração de um RIPD/DPIA.

Tanto do ponto de vista metodológico quanto do ponto de vista prático, o relatório, observado no contexto de uma adequação da empresa à lei a partir do zero, apresenta-se como um *output* que tem por entrada diversos processos que já devem estar implementados e *on-going* dentro da

organização. Seria como “começar pelo fim”, o que pode mostrar-se algo contraproducente e ineficaz. Numa abordagem mais otimista, prestar-se-ia como um instrumento de avaliação de maturidade organizacional/de processos tão-somente. Entretanto, existem ferramentas e metodologias específicas para este fim, tais como a realização de uma pré-auditoria ou um *gap assessment*. O relatório não se prestaria como o remédio mais indicado, aprioristicamente.

A Fase 2 implica uma análise às relações com terceiros, nomeadamente *joint controllers* ou processadores. No GDPR, a colaboração para DPIAs só tem força de Lei para os processadores, pelo que se sugere que num contrato junto a *joint controllers* se inclua uma cláusula para permitir essa colaboração.

A Fase 3 concentra-se em identificar os controles que já existem. Estes controles são tanto de ordem legal como de tratamento de riscos. Entram nessa categoria, portanto, todas as medidas legais, técnicas, físicas e organizacionais, que consideradas a partir do ponto de vista de assegurar ao indivíduo seus direitos previstos, já existem e como elas se relacionam ao processamento objeto do relatório. A necessidade e a proporcionalidade do processamento são verificadas, através da avaliação de medidas existentes para este fim, bem como as outras relativas à preservação dos demais direitos alcançados pela lei.

Novamente aqui faz-se necessário de que existam tais medidas para que, se necessário, sejam estas adequadas ao processamento analisado, bem como modificações a estas medidas sejam feitas, caso trate-se de uma forma nova de processamento anteriormente não prevista. Tal observação reforça a tese de que o RIPD não se presta a rigor como ferramenta de conformidade sem que sejam atendidas premissas básicas.

A Fase 4 consiste em realizar o processo de avaliação de riscos (*risk assessment*) a partir do ponto de vista do titular dos direitos. Identificar, analisar e avaliar riscos. Uma metodologia sugerida para garantir a sistematização do modelo de gestão de risco é a ISO 31000, trazendo uma padronização que confere certeza e, ao mesmo tempo,

transmite, em caso de investigação, uma forma de demonstração de compreensão e responsabilização da empresa em relação à proteção dos dados baseada numa norma adotada largamente no mercado.

O objetivo da identificação é relacionar as fontes de risco, áreas/direitos impactados, eventos e suas causas, bem como potenciais consequências. Todos os eventos e ameaças relacionadas ao processamento em análise devem ser levantados e documentados. Estes eventos podem ter origem interna ou externa, causa humana ou tecnológica, etc. Assim, a origem, natureza, particularidade, gravidade dos riscos são elencados.

Seguindo o modelo proposto, os próximos passos consistem em analisar e avaliar os riscos identificados. Ao tomar em conta os riscos aos direitos identificados no processamento, faz-se necessário, considerando os potenciais impactos nos direitos e liberdades dos titulares e ameaças aos mesmos, estimar a probabilidade e gravidade de cada um dos riscos.

A Fase 5 tem por objetivo documentar as medidas adotadas para que os riscos identificados, analisados e avaliados sejam devidamente tratados. Este tratamento pode acarretar em evitar, remover, alterar, compartilhar ou reter os riscos levantados.

Nesta fase é gerado o relatório final que resume toda a análise realizada, os controles existentes, os riscos e ameaças aos titulares, endereçando as ações a serem tomadas pela organização para cada risco, ameaça e falha identificada. Durante todo o processo a figura do Encarregado, como 2ª linha de defesa, deve ser consultado para dirimir dúvidas e receber dele eventuais sugestões/críticas/orientações.

Uma vez documentado adequadamente, o relatório deverá ser submetido aos principais gerentes das áreas afetadas da organização, para que os mesmos tomem as ações necessárias e validem o documento.
Apesar da LGPD, ao contrário do GDPR, não especificar as situações onde se faz mandatório RIPD, o legislador previu

que para os casos onde a base legal para o tratamento for o interesse legítimo, observe-se o seguinte:

Art. 10. Para os fins desta Lei, considera-se: O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercícioexercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

A Fase 6 consiste no envio do relatório ao DPO, para sua análise. O DPO fará uma análise ao DPIA e concluirá se está de acordo com o que é exigido ou se, por outro lado, há riscos que não foram corretamente mitigados ou riscos que não constam do relatório. Não havendo nada legalmente que obrigue o DPO a fundamentar a sua decisão, é boa prática que a recusa do DPO tem de ser fundamentada.

A questão mais pertinente, nestes casos, é quando o DPO rejeita o DPIA. Hipoteticamente, podemos olhar para uma empresa cujo DPO rejeitou um DPIA. A rejeição do DPO de um DPIA não é vinculativa mas deve ser tida em alta consideração, dada a especificidade do cargo. A direção da empresa, após analisar o DPIA, a opinião do DPO e os fundamentos da recusa, pode decidir avançar com o

processamento de dados, mesmo com a rejeição do DPIA pelo DPO.

No entanto, terá de fundamentar a sua decisão, visto que, em caso de investigação, ter-se-á de analisar se o risco corrido pela empresa era razoável ou negligente, colocando propositadamente em causa os direitos dos titulares de dados em seu benefício.

Outra questão coloca-se no caso do DPO aprovar o DPIA com reservas. Por exemplo, considera que o risco está convenientemente mitigado mas que a empresa pode mitigar esse risco consideravelmente com diversas e determinadas medidas técnicas e/ou organizacionais. Não sendo a forma mais comum de responder a um DPIA, não se vislumbra qualquer razão legal para que um DPO cumpra a sua função de monitorização de forma preemptiva, assinalando soluções que o DPIA não toma em consideração.

A propósito da menção feita anteriormente ao artigo 10, § 3º, a mesma é específica a um relatório idêntico ao ser gerado em qualquer outra situação onde haja riscos aos direitos dos titulares. No âmbito do GDPR porém, tem sido considerado unanimemente a necessidade de uma avaliação que fundamente o interesse legítimo, o LIA (*Legitimate Interests Assessment*).

Apesar de tratar-se de uma base legal mais flexível, o interesse legítimo não pode ser assumido como o mais apropriado por mera conveniência. O propósito do LIA é evitar que o. controlador utilize o legítimo interesse de forma arbitrária e não fundamentada, sem ter em ponderação os interesses dos titulares de dados.

A responsabilidade adicional ao agente de tratamento decorrente da utilização dessa base legal é inerente,portanto conduzir uma avaliação como um LIA pode ajudar bastante a decidir pelo legítimo interesse. Um LIA basicamente coloca de forma estruturada e documentada o teste em três partes que se recomenda ao avaliar a adequação do interesse legítimo, a saber:

Propósito | Necessidade | Balanceamento

Inicialmente, considera-se o propósito do processamento, o que se espera obter através dele:

Quem se beneficia do processamento e de que forma?

Existem benefícios públicos advindos e de que forma eles se dariam?

O quão importantes seriam esses benefícios? Etc.

Superado isso, avalia-se a real necessidade do processamento baseado em interesse legítimo:

Esse processamento de fato auxilia no propósito almejado?

Ele é indispensável?

Não haveria outra base legal possível de se utilizar para alcançar o mesmo propósito?

Há proporcionalidade entre o propósito e a necessidade?

Por fim, considera-se o impacto nos interesses, direitos e liberdades dos titulares da utilização desta base legal e são identificadas formas de mitigação do risco a esses direitos e liberdades.

Do ponto de vista prático, quando olhamos para o GDPR, um DPIA não é substituído por um LIA, mas este auxilia bastante para checar a viabilidade de se utilizar como base legal o interesse legítimo, servindo de base ao mesmo quando estão em causa processamentos que colocam direitos dos titulares de dados em risco de forma agravada. Rejeitado um LIA, não se vislumbra como se poderá avançar com o interesse legítimo como base legal.

Por último, deve-se ter em consideração que o LIA terá de ser aprovado ou rejeitado pelo DPO, com as mesmas nuances referidas supra em relação aos DPIAs.

A propósito da diferença suscitada pelo LIA entre a lei brasileira e a europeia, observa-se que no GDPR o DPIA é mandatório quando o tratamento de dados for “suscetível de implicar um elevado risco para os direitos e liberdades

das pessoas singulares" (GDPR, artigo 35.º, n.º 1).

Por outro lado, na LGPD, a abrangência não encontra premissas, ou seja, potencialmente todas as atividades de processamento, independente do grau de risco que apresentem aos direitos dos titulares, podem vir a ser demandadas pela futura autoridade de serem passíveis de RIPD por parte dos agentes de tratamento.

Ora, é fato que nossa realidade empresarial não tem ainda como foco o *compliance*, e dentro do universo da governança corporativa, a gestão de risco é antes uma exceção do que uma regra entre as empresas nacionais.

Com o advento da LGPD e com ela a demanda legal quanto a existência deste mesmo *compliance* através de controles baseados em boas práticas, é seguro dizer que no futuro tenhamos uma mudança significativa na cultura organizacional pátria. Porém, talvez não tenha sido a melhor solução deixar de modo tão "aberto" a possível necessidade de termos RIPD para todas e quaisquer situações.

Isto posto, partindo do pressuposto de que "quem pode o mais, pode o menos", segue à guisa de recomendação para a futura e tão necessária autoridade nacional que sejam adotados os mesmos critérios do GDPR quanto a necessidade de um RIPD.

Além de estarmos assim mais alinhados com a legislação que tão grande inspiração deu à LGPD, estaríamos também dando uma maior possibilidade à ANPD em tratar os casos mais críticos como devem ser tratados: prioritariamente. Ademais, por tratar-se de um órgão recém criado, e como qualquer outro, com recursos limitados, e ainda por cima num país onde não temos uma cultura como a europeia (que já dispõe de regulação na área desde a década de 90, com a Diretiva que foi substituída pelo GDPR), existe uma tendência que tenhamos uma quantidade muito grande de demandas a autoridade, em especial nos momentos iniciais de vigência da lei.

Por tratar-se de uma abordagem nova no país de garantia aos direitos relativos à privacidade e proteção de dados

pessoais, extremamente bem vinda, corre-se no entanto o risco de que, não atendendo a demanda supracitada, a ANPD venha a perder de alguma forma credibilidade e, dessa forma, tornar-se “mais uma agência”. E isto podendo vir a ocorrer justamente quando conquistamos a duras penas um patamar elevado de segurança jurídica com o advento da LGPD seria lamentável.

Assim sendo, não podemos correr o risco de termos uma das suas principais ferramentas inovadoras, a autoridade nacional, desgastada já de saída.

Tempo de guarda

Luanna Rodrigues Peporini

Tempo de guarda

Por quanto tempo os arquivos devem ser mantidos?

Ao tratarem da elaboração de avaliações de impacto da proteção de dados ou relatórios de impacto à proteção de dados pessoais, nem o GDPR e nem LGPD, respectivamente, abordam a questão dos prazos de guarda de tais avaliações ou relatórios, ou seja, por quanto tempo os controladores de dados deverão manter tais documentos em seus arquivos.

Parece-nos, claramente, que tais documentos devem ser mantidos durante todo o período durante o qual a atividade que gerou a necessidade de elaboração das avaliações ou relatórios seja praticada pelo controlador.

O maior questionamento dos controladores é o prazo de guarda dos relatórios após cessarem as atividades do controlador que deram ensejo à sua elaboração. Em princípio, como o relatório não conterá

dados pessoais, não há limite máximo de prazo para a guarda, ou seja, o controlador pode manter tais relatórios por tempo indeterminado.

A questão que se coloca, portanto, é qual o prazo necessário de guarda dos relatórios, ou seja, o prazo mínimo que os controladores devem manter tais documentos em seus arquivos. Entendemos que isso dependerá de como o controlador desenvolve suas atividades e do quanto está disposto a correr riscos.

O controlador poderia se valer de partes de um relatório validado por uma autoridade, quando aplicável, ou já utilizado para outras atividades, para o desenvolvimento de atividade nova, porém relacionada à anterior. Nesse caso, faria sentido manter todo o histórico de relatórios, já que há uma relação entre eles.

Outro aspecto fundamental a ser levado em consideração é o prazo prescricional relacionado a qualquer demanda que possa ser decorrente do relatório ou das atividades que ensejaram a sua elaboração. Ou seja, o prazo que eventual autoridade poderia sancionar o controlador, após cessada a atividade que se fundamentou no relatório, o prazo que poderão ser ajuizadas ações civis públicas relacionadas ao uso feito dos dados ou, até mesmo, o prazo para que um titular de dados ajuíze ação contra o controlador.

Nesse ponto, vale considerar que a depender da posição do titular na relação com o controlador, ou seja, consumidor, empregado etc, tal prazo será diferente.

Governança corporativa

Remi Yun

Governança corporativa

Importância do DPIA

Em razão dos efeitos da nova Lei Europeia – *General Data Protection Regulation* (GDPR), aplicação de multas milionárias têm sido testemunhadas rotineiramente, causando assim, diversas iniciativas/ações desestruturadas dentro das organizações brasileiras, já que a LGPD entrará em vigor em 2020.

Tais confusões justificam-se na ausência de uma Agência Nacional de Proteção de Dados quanto o desenvolvimento de guias ou orientações em relação as aplicações práticas dos dispositivos legais.

Uma delas se encontra no desenvolvimento do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) previsto no LGPD, pois não resta claro a função ou área responsável pelo desenvolvimento do relatório, sua periodicidade, etc.

Em busca da conformidade exigida pela nova legislação, muito se comenta que a elaboração do Relatório de Impacto se trata do primeiro documento a ser desenvolvido pela organização, mas se enganam aqueles que seguem esse entendimento, pois o presente relatório é consequência ou fruto da cultura do *Privacy by Design* (PbD) ou "Privacidade Desde a Concepção" a ser implementada dentro da organização.

O que faz sentido, já que se trata de uma metodologia na qual a proteção de dados pessoais é observada desde a concepção de sistemas, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais (Ann Cavoukian, 1990).

Diante desse contexto, tal metodologia alcançará a efetividade esperada quando estiver estruturada uma boa prática de governança corporativa devidamente alinhada numa gestão ou cultura de riscos.

Segundo IBGC, a Governança Corporativa está pautada por alguns princípios básicos que são convertidos em recomendações objetivas, tais como:

GOVERNANÇA CORPORATIVA

Princípios básicos

Responsabilidade corporativa

Prestação de Contas

Transparência

Equidade

Responsabilidade Corporativa (*Compliance*)

Os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional, etc.) no curto, médio e longo prazos.

Prestação de Contas (*Accountability*)

Os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis.

Transparência (*Disclosure*)

Consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não se limitar apenas às disposições de leis/regulamentos, ou desempenho econômico financeiro, mas deve contemplar demais fatores inclusive intangíveis que norteiam a ação gerencial, pois a adequada transparência resulta em um clima de confiança.

Equidade (*Fairness*)

Tratamento justo e isonômico de todos os sócios e demais partes interessadas.

Não restam dúvidas que os princípios básicos supracitados são condições a serem identificados numa boa governança corporativa através de uma estrutura clara e madura com as atribuições e responsabilidades de cada agente nos diferentes níveis e práticas de gestão de risco devidamente estabelecidas e formalizadas, por exemplo, quem identifica, avalia, trata os riscos, bem como quem monitora e fiscaliza o processo como um todo.

O resultado da boa governança fica atrelado ao desenvolvimento econômico sustentável de longo prazo, melhoria no desempenho das empresas, bem como o

aumento do acesso ao capital externo. A integração da cultura de risco com a governança refletirá diretamente no processo de tomada de decisão, identificando-se uma interação entre todos os níveis da organização e seus respectivos agentes dentro das linhas de defesa esperada, resguardando-se sua independência.

Para que o processo de tomada de decisão ocorra dentro das conformidades esperadas, a gestão de riscos corporativos, bem como seus monitoramentos devem ser exercidos pelas três linhas de defesa que seguem abaixo:

1ª Linha de defesa: realizada pelos gestores das unidades e responsáveis diretos pelos processos e sobre os riscos;

2ª Linha de defesa: realizada pelos gestores corporativos de gestão de riscos, conformidade (*compliance*), controle e que contempla o monitoramento de visão integrada dos riscos;

3ª Linha de defesa: realizada pela auditoria interna que fornece avaliações independentes;

Nessa estrutura, cada uma dessas três linhas desempenha um papel distinto, podendo existir várias alternativas para a construção da governança de gestão de riscos, cabendo cada organização adotar aquela mais adequada ao seu perfil e nível de maturidade.

Diante do contexto acima, é de suma importância identificar um responsável pelo desenvolvimento do Relatório de Impacto à Proteção de Dados Pessoais, dentro da estrutura das três linhas de defesas que deve seguir embasado numa cultura de riscos devidamente integrada a governança corporativas.

Neste caso, não se vislumbra outra opção além da primeira linha de defesa como sendo o responsável em desenvolver o relatório, ou seja, os próprios gestores das unidades, ora responsáveis diretos dos processos, consequentemente pelos riscos inerentes a eles, assegurando assim, a efetividade das ações adotadas quanto a cultura do *Privacy by Design* (PbD).

Tal entendimento resta fundamentado na recomendação provido pela FERMA (*The Federation of European Risk Management Associations*) ao definir a segunda linha de defesa como a estrutura em que o encarregado de dados pessoais ou *Data Protection Officer* (DPO) deveria estar enquadrado.

O que corrobora com o dispositivo do art. 41, § 2º, inciso III da LGPD que dispõem sobre as atividades do encarregado, sendo uma delas o aspecto de orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

Conclui-se que as áreas e/ou pessoas pertencentes a primeira linha de defesa tem a obrigação e responsabilidade de identificar e minimizar os riscos de proteção de dados de um projeto, tendo o dever de consultar seu encarregado ou DPO para avaliar o nível de risco mapeado e documentá-lo como parte do processo.

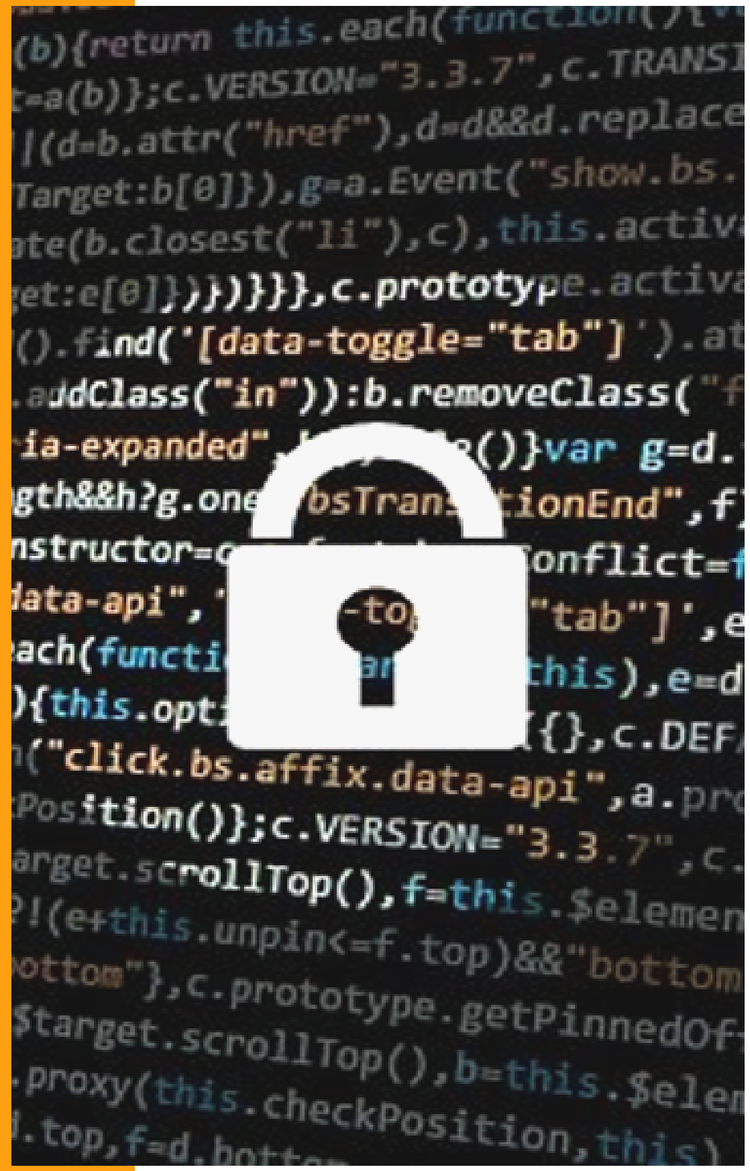
Há a possibilidade de terceirizar o relatório, mas independentemente dessa delegação, a responsabilidade

permanece para quem terceirizou. Caso haja uma operação de processamento relevante, o processador poderá elaborar o relatório quando solicitado.

Na prática haverá uma imensa confusão, pois a previsão quanto à solicitação ou consulta do encarregado não gera a presunção de responsabilidade do encarregado para elaboração do relatório de impacto.

Considerações finais

Caio César Carvalho Lima



Considerações finais

Se há algumas décadas os PIAs eram considerados apenas um meio utilizado pelas organizações para analisar e gerenciar riscos, com a entrada em vigor da LGPD e a necessidade de realização de DPIAs, estes tornar-se-ão uma exigência legal.

Assim, de uma ferramenta útil na gestão de riscos – parte da abordagem geral de uma empresa para a construção de uma imagem clara de suas atividades de tratamento de dados – passarão a ser uma verdadeira exigência de *compliance*, quando aplicável, para entender se tais atividades são arriscadas ou não. Tal documentação demonstrará, ainda, quais medidas foram adotadas para prevenir, controlar e mitigar tais riscos.

Embora os métodos para conduzir os relatórios possam variam amplamente de organização para organização, todos os seus membros deverão compreender que possuem um papel a desempenhar na entrega da estrutura de privacidade.

Assim, será necessário um olhar atento dos controladores de dados pessoais sobre a escolha da metodologia adequada para a elaboração e execução dos relatórios, seja para evitar as sanções legais em razão de seu descumprimento dentro dos casos previstos, seja para afastar danos reputacionais e perdas no retorno de investimentos resultantes da desconfiança por parte dos cidadãos.

SOBRE OS AUTORES

Relatório de Impacto à Proteção de Dados Pessoais

Caio Lima

Advogado
Mestre em Direito Processual Civil pela PUC-SP

in/caiocclima

Luanna Peporini

Advogada
Especialista em propriedade intelectual, contratos, direito digital e internet

in/luanna-rodrigues-peporini-2b2a5911

Marcílio Braz Jr.

Advogado
Especialista em privacidade e proteção de dados; fundador da Privacy Academy

in/marciliobrazjr

Maria Hosken

Advogada
Mestre em Propriedade Intelectual e Inovação pelo INPI

in/mariahosken

SOBRE OS AUTORES

Relatório de Impacto à Proteção de Dados Pessoais

Nuria Baxauli

Advogada
Especialista em
Propriedade Intelectual e
Tecnologia

in/núria-baxauli-1b0698107

Remi Yun

Advogada e Auditora
Interna
Especialista em Gestão de
Riscos, Compliance e
Investigação Forense

in/remiyun

Raphael Dutra

Advogado
Especialista em Data
Protection and Privacy

in/raphael-dutra-da-costa-campos-278362138

Referências bibliográficas

[1] CLARKE, Roger. *Privacy Impact Assessment*: *Its Origins and Development. Computer Law & Security Review 25*, 2 (April 2009) 123-135. Elsevier, 2009. Disponível em http://www.rogerclarke.com/DV/PIAHist-08.html. Acesso em 26/11/2018.

[2] "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk*." (EU Regulation 657/2016 - GDPR).

[3] "*That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation*." (EU Regulation 657/2016 - GDPR).