15° CONGESP
CONGRESSO DE GESTÃO PÚBLICA DO RIO GRANDE DO NORTE
GESTÃO PÚBLICA, DESENVOLVIMENTO REGIONAL E AS EXPERIÊNCIAS INOVADORAS DO CONSÓRCIO NORDESTE
30 nov - 03 dez | evento online

A IMPORTÂNCIA DO RELATÓRIO DE IMPACTO À PROTEÇÃO DOS DADOS PESSOAIS (RIPD) PARA SEGURANÇA DOS DADOS PESSOAIS TRATADOS NO SERVIÇO PÚBLICO

Hemily Samila da Silva Saraiva[1]

Raquel Teixeira de Brito[2]

INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei Federal nº 13.709 de 14 de agosto de 2018, entrou em vigor em 18 de setembro de 2020 e, desde de então vem produzindo efeitos tanto no âmbito público, quanto no privado, com o objetivo de tutelar dados pessoais, o que no setor público demanda esforços, haja vista que a Administração Pública precisa promover a adequação das atividades de tratamento de dados pessoais de acordo com as disposições elencadas pela LGPD, sob a possibilidade de responsabilização em caso de inadequação a tais medidas, de acordo com a penalidades que a Lei prevê[3].

A questão do vazamento de dados pessoais no setor público é algo que merece ser discutido, para que a Administração Pública não fique à mercê dessa prática. A necessidade de adequação e conformidade a LGPD é um dever dos órgãos públicos, imprescindível para que haja controle, fiscalização e a segurança de dados pessoais.

Nesse âmago, o objetivo deste trabalho é apresentar os aspectos gerais do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), documento norteador para auxiliar no processo de adequação à LGPD e as etapas de sua elaboração, com o intuito de demonstrar a importância desse instrumento para nortear a implementação da LGPD no Setor Público. Além disso, citaremos exemplos de medidas a serem abordadas em RIPD's, com vistas a

---

[1] Advogada. Pesquisadora-bolsista da Escola de Governo do Estado do Rio Grande do Norte. Mestranda em Constituição e Garantia de Direitos e Especialista em Direito Administrativo pela Universidade Federal do Rio Grande do Norte – UFRN. Especialista em Direito Civil e Empresarial pela Universidade Potiguar – UNP e Especialista em Processo Civil pelo Centro Universitário do Rio Grande do Norte – UNI/RN. Membro do Instituto de Direito Administrativo Seabra Fagundes (IDASF). E-mail: saraivahemily@gmail.com.

[2] Advogada. Pesquisadora-bolsista da Escola de Governo do Estado do Rio Grande do Norte. Especialista em Direito Civil e Processo Civil pela Universidade Futura. Habilitada em Direito do Petróleo, Gás Natural e Biocombustíveis pela Agência Nacional do Petróleo - ANP. Graduada em Direito pela Universidade Federal do Rio Grande do Norte - UFRN. E-mail: raquel.brito.424@ufrn.edu.br.

[3] SARAIVA, Hemily Samila da Silva; BRITO, Raquel Teixeira de. A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO SETOR PÚBLICO. 14º CONGESP - Congresso de Gestão Pública do Rio Grande do Norte, 2020.

conferir maior segurança ao tratamento de dados e, consequentemente, minimizar os riscos do tratamento de dados.

PROCEDIMENTOS METODOLÓGICOS

Utiliza-se para o desenvolvimento do presente trabalho, será utilizada como metodologia a revisão bibliográfica, a partir de livros, de cartilhas, de artigos científicos e da legislação. A abordagem de tais meios de pesquisa se dará de forma qualitativa e nível de investigação descritivo, uma vez que buscará, por intermédio de uma interpretação e compreensão do problema posto à luz da literatura examinada, extrair conclusões pautadas em conceitos e teorias.

O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) ou *data protection impact assessement* (DPIA) é um documento essencial para auxiliar no processo de adequação à LGPD. Tal documento está previsto no art. 5º da LGPD[4] e tem por finalidade mostrar os dados pessoais que são tratados e quais as medidas são adotadas para a mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Segundo o inciso XVII, art. 5º. da LGPD, o RIPD é um documento que deve ficar sob a custódia do Controlador dos dados pessoais, devendo conter 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. A figura do Controlador é definida como "pessoa, natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais" (LGPD, art. 5º, VI).

O RIPD deve abarcar conteúdos mínimos exigidos pela LGPD contendo 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", conforme dispõe o § único do art. 38 da LGPD.

Logo, considerando a complexidade do RIPD, faz-se importante abordar as etapas de elaboração desse tipo de documento, bem como os instrumentos auxiliares que podem ser utilizados para coletar os dados que farão parte do RIPD, como por exemplo, uma planilha de controle de atos.

ETAPAS DE ELABORAÇÃO DO RIPD

[4] 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".

Antes do tratamento de dados pessoais, deve ser elaborado o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), preferencialmente na fase inicial do programa ou projeto que tem o propósito de usar esses dados. Essas etapas foram definidas com base no Guia de Boas Práticas da LGPD[5] e no caderno da ENAP.[6]

A primeira etapa consiste em identificar os Agentes de Tratamento (controlador e operador) e o Encarregado de dados. A atenção que se deve ter nessa etapa é saber identificar quem são esses sujeitos e suas respectivas funções.

Na segunda etapa, busca-se identificar a necessidade de elaborar ou atualizar o Relatório. Inicialmente, deve-se avaliar no órgão público os programas, sistemas de informação ou processos existentes ou a serem implementados que geram impactos à proteção dos dados pessoais. Além disso, a LGPD especifica os casos facultativos e obrigatórios para avançar na real necessidade do RIDP[7].

A terceira etapa consiste em descrever o tratamento de dados, para subsidiar avaliação e tratamento de riscos. Sabendo a natureza (como o órgão público pretende tratar os dados pessoais), o escopo (representa a abrangência do tratamento de dados), o contexto (observar fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados) e finalidade (motivo pelo qual se deseja tratar os dados pessoais) do tratamento dá-se uma visão geral desse processo[8].

A quarta etapa, Identificar Partes Interessadas Consultadas, isto é, devem ser identificadas e ouvidas as partes relevantes no processo de tratamento dos dados pessoais, de forma a analisar as opiniões trazidas acerca dos aspectos legais, técnicos e administrativos na atividade de tratamento.

A quinta etapa, descrever necessidade e proporcionalidade, se pauta no art. 6º, III da Lei, no qual consiste na "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

---

[5] BRASIL. Governo Federal. GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Guia de Boas Práticas para Implementação na Administração Pública Federal. Ago., 2020.

[6] BRASIL. Proteção de Dados Pessoais no Serviço Público. Relatório de Impacto à Proteção de Dados Pessoais - módulo 4. Escola Nacional de Administração Pública (ENAP); Brasília, 2019.

[7] Casos específicos previstos pela LGPD em que o RIPD pode ser solicitado: Art. 4, III e §3º; Art. 10, § 3º; Art. 31; Art. 32 e Art. 38. E, por fim, casos em que há necessidade de elaborar o relatório: art. 5º, II; art. 20; art. 14; art. 42; art. 4º, § 3º; art. 10, § 3º; Uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais sensíveis ou não sejam ou devam ser tratados; art. 12 § 2º; Monitoramento sistemático de local publicamente acessível em larga escala; Alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados etc; Reformas administrativas que implicam nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades. BRASIL. Proteção de Dados Pessoais no Serviço Público. Relatório de Impacto à Proteção de Dados Pessoais - módulo 4. Escola Nacional de Administração Pública (ENAP); Brasília, 2019, p. 7-9.

[8] BRASIL. Proteção de Dados Pessoais no Serviço Público. Relatório de Impacto à Proteção de Dados Pessoais - módulo 4. Escola Nacional de Administração Pública (ENAP); Brasília, 2019, p. 9-14.

A sexta etapa é a que identifica e avalia os riscos, o art. 5º, XVII da Lei preconiza que o RIDP deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco". Nesse sentido, identifica-se os riscos que geram impacto potencial sobre o titular dos dados pessoais e a partir de cada risco identificado, define-se: "a probabilidade de ocorrência do evento de risco e o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento"[9][10].

Portanto, é importante expor ao órgão público, de forma periódica, uma análise e avaliação de riscos dos recursos de processamento da informação, sistemas de segurança da informação e quaisquer outros ativos relacionados à solução de tecnologia da informação e comunicação. Dessa forma, será indicado o nível de risco ao qual a solução e o órgão contratante estão expostos, baseado em análise de vulnerabilidades, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pelo órgão[11].

Ressalta-se, ainda, que o gerenciamento de riscos relacionado com o tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão, preconizada pela MP/CGU nº 1/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal[12].

A sétima etapa diz respeito ao art. 46 da LGPD, que significa identificar medidas para tratar os riscos atinentes a medidas de segurança, técnicas e administrativas que sejam aptas a "proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

A penúltima etapa é aprovar o Relatório, formalizando, por meio da obtenção das assinaturas do responsável pela elaboração do RIPD e pelas autoridades que representam o controlador e operador, a aprovação.

E, por fim, a última etapa do RIDP é manter a revisão. Deve ser revisto e atualizado sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais no

---

[9] BRASIL. Proteção de Dados Pessoais no Serviço Público. Relatório de Impacto à Proteção de Dados Pessoais - módulo 4. Escola Nacional de Administração Pública (ENAP); Brasília, 2019, p. 18.

[10] Para maior aprofundamento sobre gestão de risco, podem ser observadas no Manual de Gestão de Riscos elaborado pela AECI-MP que apresenta a Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão - MP, no contexto do Modelo desenvolvido no MP (Política, Instâncias de Supervisão e Metodologia). Disponível em: https://www.aneel.gov.br/documents/653889/19966798/Manual+Riscos+Estrat%C3%A9gico/a06676a2-5f6a-a700-4ba6-9d108cb204a2. Acesso em: 07 nov. 2021.

[11] BRASIL, Governo Federal. GUIA DE BOAS PRÁTICAS PARA ESPECIFICAÇÃO DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO EM CONTRATAÇÕES DE TECNOLOGIA DA INFORMAÇÃO. Brasília, setembro de 2020.

[12] BRASIL. Instrução Normativa Conjunta - MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO e a CONTROLADORIA-GERAL DA UNIÃO - MP/CGU nº 1, de 10 de maio de 2016. Disponível em: https://wiki.cgu.gov.br/index.php/Instru%C3%A7%C3%A3o_Normativa_Conjunta_MP-CGU_n%C2%BA_01,_de_10_de_maio_de_2016. Acesso em: 07 nov. 2021.

órgão público.

Como visto, o RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como aborda medidas, salvaguardas e mecanismos de mitigação de risco. Nesse sentido, sugere-se, como medidas para analisar eventuais riscos que o setor público possa vir a incorrer durante o tratamento de dados, a elaboração de uma Planilha de Controle[13] com o intuito de obter maior nível de segurança no tratamento de dados:

Imagem: Tabela de Controle para coleta de dados do RIPD

ID	CONTROLE
MEDIDA DE SEGURANÇA: POLÍTICA DE SEGURANÇA	
1	Há uma Política de Segurança Cibernética (PSC) ou equivalente publicada, incluindo Políticas ou Normas para Proteção de Dados Pessoais (PPD)?
2	Existe e é executado um processo de análise crítica da PSC e das normas ou PPD devidamente formalizado?
MEDIDA DE SEGURANÇA: GESTÃO DE RISCOS	
1	É realizada periodicamente uma análise/avaliação de riscos dos recursos de processamento da informação, sistemas de segurança cibernética e quaisquer outros ativos considerados críticos, indicando o nível de risco ao qual a aplicação e a organização está exposta e considerando a identificação das ameaças aplicáveis e análise de impacto nos negócios?
MEDIDA DE SEGURANÇA: SEGURANÇA NAS OPERAÇÕES	
1	Há projeções de capacidade futura que consideram os requisitos de novos negócios e sistemas, as tendências de utilização e as tendências atuais e projetadas de capacidade de processamento de informação da organização?
2	Há mecanismos para monitoramento do uso dos recursos, de forma a atender as necessidades de capacidade futura e garantir o desempenho requerido das aplicações?
3	São implementados mecanismos e procedimentos para evitar ataques de negação de serviço, tais como balanceamento de carga, IPS, proxy, firewall, etc.?
MEDIDA DE SEGURANÇA: ORGANIZAÇÃO DA SEGURANÇA	
1	Há uma matriz de responsabilidades com atribuição das responsabilidades pela segurança cibernética na organização, de forma a evidenciar a segregação de funções e assegurar que colaboradores e partes externas entendam suas responsabilidades?

CONCLUSÃO

[13] Modelo de Planilha de Controle formulado pelas autoras, abordando medidas de segurança que irão integrar o RIPD.

A LGPD foi um marco normativo à proteção de dados pessoais, estabelecendo, desde 2018, regulamentação sobre o tratamento e compartilhamento de dados, com a finalidade de tutelar esses dados, coibindo o vazamento e uso indevido deles. A não conformidade à legislação pode trazer diversos problemas à Administração Pública, daí a adequação ser uma necessidade, no qual o setor público e privado não podem se eximir.

Para perseguir o objetivo de implementação da LGPD o Encarregado da Proteção de Dados precisa elaborar um RIPD, documento essencial para auxiliar no processo de adequação à LGPD. Como abordado neste trabalho o RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos à segurança e privacidade de dados pessoais sensíveis, bem como aborda medidas, salvaguardas e mecanismos de mitigação de risco. Por isso, é tão importante se ter controle, como o que pode ser feito por meio de tabelas de controle, a exemplo da que foi apresentada neste trabalho.

Portanto, podemos concluir que o setor público, no exercício de suas funções, especificamente no tratamento de dados pessoais, deve seguir e ajustar suas condutas junto ao RIPD, buscando as melhores soluções e segurança à atividade de tratamento de dados, com vistas a garantir segurança aos dados e mitigar os riscos dessa atividade.

REFERÊNCIAS

BRASIL. Governo Federal. GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Guia de Boas Práticas para Implementação na Administração Pública Federal. Ago., 2020.

BRASIL. Proteção de Dados Pessoais no Serviço Público. Relatório de Impacto à Proteção de Dados Pessoais - módulo 4. Escola Nacional de Administração Pública (ENAP); Brasília, 2019.

BRASIL. Instrução Normativa Conjunta - MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO e a CONTROLADORIA-GERAL DA UNIÃO - MP/CGU nº 1, de 10 de maio de 2016. Disponível em: https://wiki.cgu.gov.br/index.php/Instru%C3%A7%C3%A3o_Normativa_Conjunta_MP-CGU_n%C2%BA_01,_de_10_de_maio_de_2016. Acesso em: 07 nov. 2021.

BRASIL, Governo Federal. GUIA DE BOAS PRÁTICAS PARA ESPECIFICAÇÃO DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO EM CONTRATAÇÕES DE TECNOLOGIA DA INFORMAÇÃO. Brasília, set. de 2020.

SARAIVA, Hemily Samila da Silva; BRITO, Raquel Teixeira de. A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO SETOR PÚBLICO. 14º CONGESP - Congresso de Gestão Pública do Rio Grande do Norte, 2020.