UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
ESCOLA DE INFORMÁTICA APLICADA

ANÁLISE DOS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS SOBRE A GOVERNANÇA E SEGURANÇA DE DADOS

JULIANA GONÇALVES DOS SANTOS
SABRINA LAPA DA COSTA E SILVA

Orientador
Asterio Kiyoshi Tanaka

RIO DE JANEIRO, RJ – BRASIL
FEVEREIRO DE 2020

Catalogação informatizada pelo autor

C837 Costa e Silva, Sabrina Lapa da
Análise dos impactos da Lei Geral de Proteção de Dados Pessoais sobre a governança e segurança de dados / Sabrina Lapa da Costa e Silva. -- Rio de Janeiro, 2020.
48p

Orientador: Asterio Kiyoshi Tanaka.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Estado do Rio de Janeiro, Graduação em Sistemas de Informação, 2020.

1. LGPD. 2. Proteção de dados. 3. Governança. 4. Segurança da Informação. 5. Incidentes. I. Tanaka, Asterio Kiyoshi, orient. II. Título.

S237 Santos, Juliana Gonçalves dos
Análise dos impactos da Lei Geral de Proteção de Dados Pessoais sobre a governança e segurança de dados / Juliana Gonçalves dos Santos. -- Rio de Janeiro, 2020.
48p

Orientador: Asterio Kiyoshi Tanaka.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal do Estado do Rio de Janeiro, Graduação em Sistemas de Informação, 2020.

1. LGPD. 2. Proteção de dados. 3. Governança. 4. Segurança da Informação. 5. Incidentes. I. Tanaka, Asterio Kiyoshi, orient. II. Título.

ANÁLISE DOS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS SOBRE A GOVERNANÇA E SEGURANÇA DE DADOS

JULIANA GONÇALVES DOS SANTOS
SABRINA LAPA DA COSTA E SILVA

Projeto de Graduação apresentado à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) para obtenção do título de Bacharel em Sistemas de Informação.

Aprovado por:

_____

Asterio Kiyoshi Tanaka (UNIRIO)

_____

Morganna Carmem Diniz (UNIRIO)

_____

Reinaldo Viana Alvares (UNIRIO)

RIO DE JANEIRO, RJ – BRASIL
FEVEREIRO DE 2020

Agradecimentos

Agradecemos a Deus que nos deu força e nos permitiu realizar esse sonho. Somos gratas aos nossos familiares que nos apoiaram até aqui e que foram a nossa fonte de inspiração. Somos gratas aos amigos que não deixaram o cansaço nos vencer. Aos nossos mestres que acompanharam toda a nossa trajetória dentro do curso, principalmente ao nosso orientador, Asterio Tanaka, que foi incansável em suas orientações, pesquisas e revisões. Nosso muito obrigado à UNIRIO por nos proporcionar o melhor ambiente educacional.

RESUMO

Já há algum tempo, a informação é um dos ativos mais valiosos dentro das organizações. Seja no que diz respeito a documentos digitais, recursos de projetos ou dados de clientes e colaboradores, sua perda ou vazamento pode representar um prejuízo irreparável ou até mesmo exposição negativa da empresa, o que explica a importância da segurança da informação. Devido aos riscos gerados por ataques, pelos números de incidentes com segurança da informação, a necessidade de garantia de integridade e disponibilidade dos dados, a carência de manutenção para o bom andamento do negócio e a falta de confiança de clientes e investidores foi criada uma lei, a LGPD – Lei Geral de Proteção de Dados Pessoais - 13.709/2018, que regulamenta o uso, a proteção e a transferência de dados pessoais de indivíduos localizados em território brasileiro, garantindo o direito à privacidade e a proteção destes. Este trabalho aborda de forma abrangente os impactos da LGPD, comentando sobre os principais assuntos, como: a necessidade de mapeamento dos dados, a importância de um encarregado de proteção de dados, gestão dos incidentes, segurança desses dados, sanções e multas. Com o entendimento da lei, percebe-se que dedicar esforços para implantar a governança de dados e a segurança da informação, tendo ciência das implicações nas empresas, é um investimento necessário para manter seus dados a salvo, adotando medidas de segurança, técnicas e administrativas para proteção dos dados pessoais de acessos não autorizados e protegendo a informação durante todo o ciclo de vida.

Palavras-chave: LGPD, proteção de dados, governança, segurança da informação, incidentes.

ABSTRACT

For some time now, information has been one of the most valuable assets within organizations. Whether it is digital documents, project resources, or customer and employee data, their loss or leakage can be irreparable damage or even negative company exposure, which explains the importance of information security. Due to the risks posed by attacks, the number of information security incidents, the need to ensure data integrity and availability, the lack of maintenance for the smooth running of the business and the lack of trust of clients and investors, a law has been created, LGPD - General Law on Personal Data Protection - 13.709 / 2018, which regulates the use, protection and transfer of personal data of individuals located in Brazilian territory, guaranteeing their right to privacy and protection. This paper addresses the impacts of LGPD comprehensively, commenting on key issues such as the need for data mapping, the importance of a data protection officer, incident management, data security, sanctions and fines. With the understanding of the law, it is clear that dedicating efforts to implement data governance and information security, being aware of the implications for companies, is a necessary investment to keep your data safe, adopting security, technical and administrative measures for protecting personal data from unauthorized access and protecting information throughout the life cycle.

Keywords: LGPD, data protection, governance, information security, incidents.

SUMÁRIO

ÍNDICE DE FIGURAS

1. Introdução

1.1 Motivação

A dependência da tecnologia torna-se cada vez maior quando observado o aumento da velocidade de demanda no mundo. Para ser competitivo no mercado, é quase que obrigatório o compartilhamento de informações com os fornecedores, parceiros e clientes. Em meio a esse rápido fluxo de informações, faz-se necessária a atualização de meios ágeis e sistemas automatizados, como softwares modernos. Uma preocupação, que pode-se dizer que estava um pouco negligenciada, é a vulnerabilidade do tratamento e armazenamento de informações (CABRAL; CAPRINO, 2015).

Dados pessoais são considerados valiosos e de extremo sigilo. Com o aumento da utilização de dados para infinitas finalidades de diversas entidades, surge a necessidade de uma regulamentação específica da utilização desses dados, com o objetivo de prevenir crime por exposição de informação sigilosa e, por conseguinte, proteger os direitos fundamentais de liberdade e privacidade.

Em 14 de agosto de 2018 foi sancionada a Lei n°13.709/18 chamada Lei Geral de Proteção a Dados Pessoais (LGPD), que entrará em vigor no mesmo período do ano de 2020, após vinte e quatro meses de *vacatio legis* (termo jurídico sobre o tempo decorrido entre o dia da publicação de uma lei e o dia em que seu cumprimento torna-se obrigatório). Quando estiver vigente, essa lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, irá estabelecer uma série de regras que empresas e outras organizações atuantes no Brasil terão que seguir.

O objetivo principal da LGPD é permitir que o cidadão tenha mais controle sobre o tratamento que é dado às suas informações pessoais. Desta forma, cidadãos, consumidores e titulares passam a ter confiança na coleta, uso e privacidade de seus dados. Quanto às empresas, novas normas ficam estabelecidas para definir com mais

clareza o tratamento, armazenamento, coleta e segurança de compartilhamento desses dados. Portanto, a instauração dessa lei estabelecerá exigências e determinará penalidades para maior segurança no âmbito jurídico e, consequentemente, desenvolvimento econômico e tecnológico da sociedade. “Seu principal objetivo é aumentar a autonomia do titular sobre as próprias informações [...] Isso obriga as empresas a incrementar a proteção desses dados” (GLAB PARA MICROSOFT, 2019).

A lei impacta profundamente a gestão dos dados pessoais pelas empresas de todos os setores e, portanto, muitas instituições iniciaram uma corrida de vinte e quatro meses para adequarem seus processos e sistemas de informação às novas obrigações. Nessa jornada de conformidade, as empresas terão que implementar novos procedimentos e provavelmente novos departamentos, conforme o caso, para alinhar-se às normas (POHLMANN, 2019).

O assunto ainda é muito recente no Brasil, existe pouco aprofundamento sobre o tema com foco na governança e segurança de dados, faltando detalhes e materiais para consulta pelos que tentam se adequar. Em maio de 2019, foi realizado no Superior Tribunal de Justiça (STJ), em Brasília, um seminário internacional com o objetivo de debater a implantação da LGPD no Brasil. Membros do governo e Congresso Nacional discutiram ordenamentos e análises de práticas internacionais cabíveis. Na busca por mais conteúdo sobre o assunto, as discussões do simpósio serão reunidas em uma obra coletiva publicada (CONSELHO DA JUSTIÇA FEDERAL, 2019).

Para entrar em conformidade com a nova lei, além dos aspectos jurídicos, existem dois principais pilares tecnológicos que as empresas precisam avaliar internamente para alcançarem o mínimo exigido pela LGPD: governança de dados e segurança da informação. De acordo com o artigo 50, os controladores e operadores “poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização [...] e outros aspectos relacionados ao tratamento de dados pessoais” (BRASIL, 2018). Já o artigo 46 da lei determina que “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados [...] ou qualquer forma de tratamento inadequado ou ilícito” (BRASIL, 2018). Por fim, o artigo 9 retrata que “o

titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva" (BRASIL, 2018).

Apesar do que era acreditado, as estatísticas mostram que as empresas brasileiras aparentam não ter preocupações com a nova lei. Segundo pesquisa da consultoria ICTS Protiviti, divulgada em novembro de 2019 pela revista Época Negócios Online, 84% das companhias brasileiras ainda não estão em conformidade com as novas regras de privacidade de dados.

> Segundo o relatório, apenas 12,5% das empresas afirmam ter feito mapeamento de risco de segurança da informação e proteção de dados - etapa primária para adequação à lei. Apenas 17,3% se dizem preparadas para fazer a gestão da privacidade de dados processados por seus fornecedores e terceiros. [...] O relatório da ICTS Protiviti reuniu as informações durante agosto e novembro deste ano de 104 empresas, das quais 33% são de grande porte, 27,5% médias e 39,6% são micros e pequenas empresas. Os setores das organizações são variados, como varejo, construção, saúde, educação, telecomunicação, tecnologia da informação, indústria, entre outros. (ÉPOCA NEGÓCIOS ONLINE, 2019).

Entretanto, as penalidades previstas a quem descumprir as diretrizes da LGPD são preocupantes. Dentre as punições, a multa por descumprimento pode chegar a 2% do faturamento da empresa em seu último exercício fiscal, limitada a 50 milhões de reais (EXAME, 2019).

Com esse cenário, muitas companhias de consultoria estão explorando as demandas do mercado e estão oferecendo assistência para a adequação de empresas brasileiras às normas da LGPD.

1.2 Objetivo

O presente trabalho visa abordar os impactos da LGPD na governança e segurança de dados dentro das empresas brasileiras, com foco no capítulo VII desta lei – capítulo que retrata da segurança, sigilo de dados, boas práticas e governança. Também serão abordados outros aspectos relevantes da LGPD. Através da análise das normas da ISO 27001 – Sistema de Gestão de Segurança da Informação, podem-se identificar requisitos mínimos obrigatórios que uma empresa deve ter para estar em conformidade com a lei.

1.3 Organização do texto

O texto está estruturado em capítulos e, além desta introdução, será desenvolvido da seguinte forma:

- Capítulo II: Revisão Teórica - contém uma revisão bibliográfica sobre a Lei Geral de Proteção de Dados Pessoais. Trata o surgimento e conceituação da lei, passando pelos principais aspectos e as penalidades previstas.

- Capítulo III: Governança de dados - análise dos impactos da lei nas organizações, com foco nas atividades de planejamento, monitoramento e execução.

- Capítulo IV: Segurança de dados - avaliação dos aspectos mínimos que uma organização deve conter para estar em conformidade com a lei, com base na norma ISO 27001, incluindo análise dos conceitos expostos e resultados obtidos.

- Capítulo V: Conclusões - reúne as considerações finais, assinala as contribuições da pesquisa e sugere possibilidades de aprofundamento posterior.

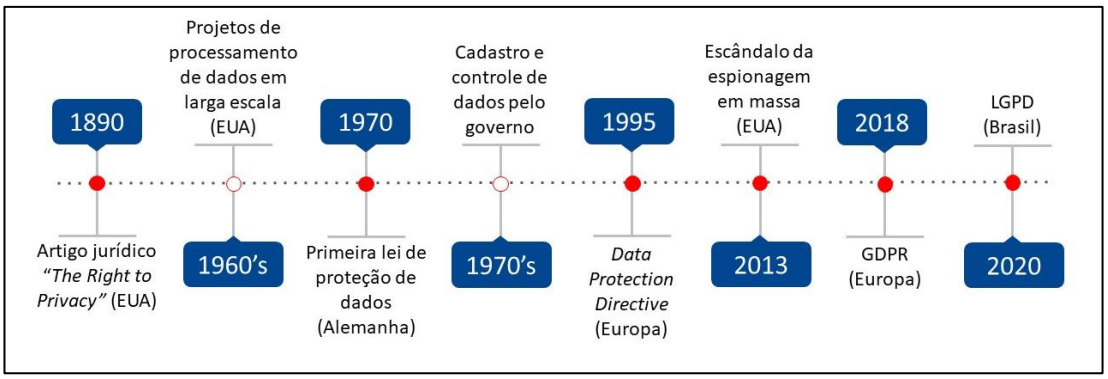
Importante ressaltar que, apesar dos tópicos Governança de dados e Segurança de dados estarem em capítulos segregados, ambos temas são estreitamente relacionados. Essa separação foi realizada apenas para facilitar a organização do texto e das ideias apresentadas.

2. Revisão teórica

2.1 O surgimento pela necessidade de segurança de dados pessoais

A linha do tempo na figura 1 ilustra os acontecimentos que desencadearam a necessidade de uma lei de proteção de dados no Brasil.

Figura 1 – Acontecimentos que influenciaram o surgimento da LGPD



Fonte: Autoria própria

Com o advento das tecnologias da informação, a proteção da privacidade individual passou a ser uma preocupação jurídica, a ser analisada como um dos direitos da personalidade. No entanto, o assunto só tomou forma a partir da década de 60, com o surgimento dos primeiros projetos de processamento de dados em larga escala e de forma centralizada. Esses projetos iniciados nos Estados Unidos desencadearam uma demanda por leis específicas para regular a coleta, armazenamento e manuseio de dados pessoais. Em 1890, Samuel Warren e Louis Brandeis publicaram o artigo jurídico *The Right to Privacy* na revista *Harvard Law Review*. Esta obra é um dos marcos mais influentes na história dos Estados Unidos e é amplamente reconhecida como a primeira publicação do país sobre a defesa do direito à privacidade, inaugurando o conceito "direito de ser deixado só" (*right to be let alone*). (WARREN; BRANDEIS, 1890).

Apesar dos primeiros passos serem norte-americanos, a primeira lei de proteção de dados foi uma lei estadual criada em Hesse na Alemanha, em 1970. O propósito era proteger todos os dados digitalizados de órgãos públicos (titularidade pública) contra divulgação, tratamento indevido, alteração ou exclusão por funcionários públicos (RULE; GREENLEAF, 2010). Desde então, a Europa iniciou um movimento de elaboração de leis estaduais e federais de proteção às informações de pessoas físicas e, em alguns países, estenderam a regulamentação também para as pessoas jurídicas.

> Embora o "direito à privacidade" (right to privacy) tenha se desenvolvido originalmente na jurisprudência e doutrina norte-americanas, foi a Europa que se notabilizou como a fonte dos principais e mais completos conjuntos de leis sobre proteção de dados pessoais, que emergiram nessas décadas. [...] Atualmente, uma expressiva parte dos países europeus possui leis de proteção de dados, incluindo a Áustria, Bélgica, República Checa, Finlândia, Hungria, Irlanda, Itália, Luxemburgo, Holanda, Suécia, Suíça e Inglaterra (REINALDO FILHO, 2013).

Segundo o advogado Gilberto M. de Almeida, consultor das Nações Unidas sobre leis para a Internet e fundador do Instituto de Direito e Tecnologia (IDTEC), a evolução das legislações de proteção de dados pessoais ocorreu em três ondas (informação verbal)[1]:

1) Nos anos 70, na época dos *mainframes*, toda a base de dados que continha dados pessoais precisava ser cadastrada pelo governo. O volume de negócios era tão menor que autoridades do governo tinham condições de exigir que tudo fosse cadastrado e ficasse sob controle do governo (controle *a priori)*.

2) Depois nos anos 90, com o momento exponencial dos negócios e impactos da tecnologia, abandonou-se a ideia de cadastrar todos os dados e passou-se a adotar uma filosofia do controle *a posteriori*, por meio de critérios.

3) E agora com a influência da principal lei de proteção de dados da Europa, a GDPR (*General Data Protection Regulation* ou Regulamento Geral de Proteção de Dados, em português), e por conta das novas tecnologias, é necessário ter uma harmonização de plataformas e um controle integrado.

[1] Notícia fornecida por Gilberto Martins de Almeida na palestra do Fórum de Desenvolvimento do Estado do Rio de Janeiro com o tema “Lei Geral de Proteção de Dados e os impactos na relação entre empresas e consumidores”, no Rio de Janeiro, em maio de 2019.

A GDPR é considerada como uma atualização de outra lei de privacidade da Europa, chamada *Data Protection Directive* (Diretrizes para Proteção de Dados, em tradução livre), em vigência desde 1995. Foi necessário elaborar uma nova lei devido ao enorme crescimento de empresas de negócios baseados na Internet. A antiga lei não cobria totalmente os aspectos de proteção de dados, pois não abordava a dinâmica atual dos dados em redes (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2018, p. 29). A GDPR, portanto, entrou em vigor na União Europeia em 25 maio de 2018. Um dos principais fatores que impulsionaram a aprovação da lei europeia foi o escândalo da espionagem em massa promovida pelo governo dos Estados Unidos, que compartilhava informações da população americana e de vários países da Europa e da América Latina - entre eles o Brasil - utilizando servidores de empresas como Google, Apple e Facebook. “Revelado em 2013 por Edward Snowden, ex-analista da CIA, o escândalo ajudou a impulsionar a revisão da lei que havia começado no ano anterior” (GOMES, 2018).

Inicialmente, a GDPR impactava apenas empresas europeias, ou atuantes no continente ou que trabalham com dados de cidadãos europeus. No entanto, muitas empresas estão estendendo a proteção de informação pessoal a todos os seus usuários, independentemente do país de origem. Os efeitos dessa norma europeia no Brasil foram quase que imediatos, uma vez que toda e qualquer companhia que manipulava dados e informações de cidadãos europeus precisou atualizar-se perante as exigências.

A abrangência da GDPR atravessa fronteiras geográficas, com seu impacto principalmente em atividades multinacionais em todo o mundo. Afinal, qualquer empresa que contenha dados de cidadãos de países da União Europeia, mesmo que esteja localizada em outro país, está sujeita a essa regulamentação.

> Seu impacto (GDPR) já é sentido em escala mundial. Dessa forma, adequar-se à nova política tornou-se uma obrigação. Ainda assim, seria tecnicamente inviável modificar as políticas de dados apenas para os territórios da União Europeia, sem modificar nos outros. Por isso, as empresas optaram por realizar alterações a nível global ao invés de apenas na Europa (REDAÇÃO JURIS CORRESPONDENTE, 2018).

O Brasil recebeu uma forte pressão para atender ao novo nível de exigências nas práticas de tratamento de dados pessoais. A redação da lei brasileira foi fortemente inspirada na GDPR e traz em si uma semelhança considerável. Foram em

torno de oito anos de debates e redações legislativas até que a LGPD fosse sancionada.

2.2 Principais aspectos da LGPD

A LGPD exigirá mudanças extensivas nos processos e atividades empresariais que envolvem dados pessoais, cujo objetivo é proteger os direitos de liberdade e de privacidade, assegurando o livre desenvolvimento da personalidade da pessoa natural.

Uma questão bastante relevante refere-se aos tipos de dados abrangidos pela LGPD. Para os fins desta lei, considera-se: "dado pessoal – que não se refere simplesmente aos dados de pessoa natural identificada, mas também de pessoa identificável por algum meio; dado pessoal sensível – diretamente influenciada pela GDPR e que só havia sido mencionada em legislação brasileira específica pela Lei do Cadastro Positivo, portanto restrito ao contexto da concessão de crédito; dado anonimizado – relativo a titular que não possa ser identificado; e consentimento – termo de grande importância jurídica, que aparece trinta e seis vezes no texto da lei (incluindo uma vez o verbo consentir)" (TANAKA, 2019).

Percebe-se que a LGPD possui um conceito amplo dos dados pessoais, sem uma lista definitiva, o que dá maior longevidade à lei e deixa a definição da sua amplitude para os reguladores e os agentes de tratamento. Contudo, não é qualquer dado que será objeto de regulação pela LGPD, somente os dados estabelecidos pela lei e denominados Dados Pessoais.

A lei também possui uma definição ampla em relação ao escopo e abrangência territorial. Segundo o artigo 5º, Inciso X, da LGPD, tratamento de dados pessoais é "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018). Nota-se uma conceituação bastante genérica que impactará a totalidade das companhias, de pequeno a grande porte dos mais diversos setores e ramos, desde instituições financeiras até hotelaria em pontos turísticos;

quando utilizarem qualquer registro de dados de clientes, funcionários, fornecedores, prestadores de serviço, entre outros.

O artigo 3º define sua abrangência territorial, pois estabelece que ela se aplica "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados" (BRASIL, 2018). Isso significa que não importa onde os dados estão armazenados ou onde a empresa está localizada, a lei engloba todo tratamento de dados de pessoas naturais localizadas em território brasileiro.

Outro importante aspecto da LGPD são os direitos dos titulares dos dados. Titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. A lei estabelece que o titular tem o direito de:

- Confirmação da existência de tratamento e acesso a todos os seus dados pessoais que estão sendo coletados e tratados;
- Retificação de dados incompletos, inexatos ou desatualizados;
- Restrição de tratamento de dados pessoais, através da recusa em fornecer o consentimento;
- Cancelamento ou exclusão de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- Transferência dos seus dados pessoais de um controlador para outro;
- Revogação de consentimento para o tratamento de seus dados pessoais a qualquer momento, bastando uma manifestação expressa, por procedimento gratuito e facilitado;
- Oposição a quaisquer tratamentos e informações que não estejam em conformidade com a lei;
- Recebimento de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo controlador para a tomada de decisão com base em tratamento automatizado de dados pessoais;

- Recebimento de informações sobre as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

A LGPD impõe penalidades graves por descumprimento das diretrizes definidas, tornando-se um dos mais influentes impactos da sua aplicação, além de facilitar a adesão das empresas às novas exigências. Entretanto, a sociedade civil e os legisladores brasileiros entendem que as empresas não estão dando a devida atenção às responsabilidades de conformidade com a proteção de dados pessoais. É cada vez mais frequente a ocorrência de incidentes de uso indevido de dados - como o caso do Facebook e Cambridge Analytica ocorrido em 2018 - e vazamentos por negligência – caso Yahoo em 2014.

> [...] as sanções e penalidades buscam estimular as empresas a qualificar suas políticas e processos direcionados a privacidade e proteção dos dados. A LGPD impõe multas para cada infração de até 2% do faturamento limitadas a R$ 50 milhões (artigo 52, parágrafo II), números que buscam chamar a atenção da alta direção das instituições e provocar um movimento ativo na busca de melhores ações de governança de dados pessoais e privacidade (SISQUALIS, 2019).

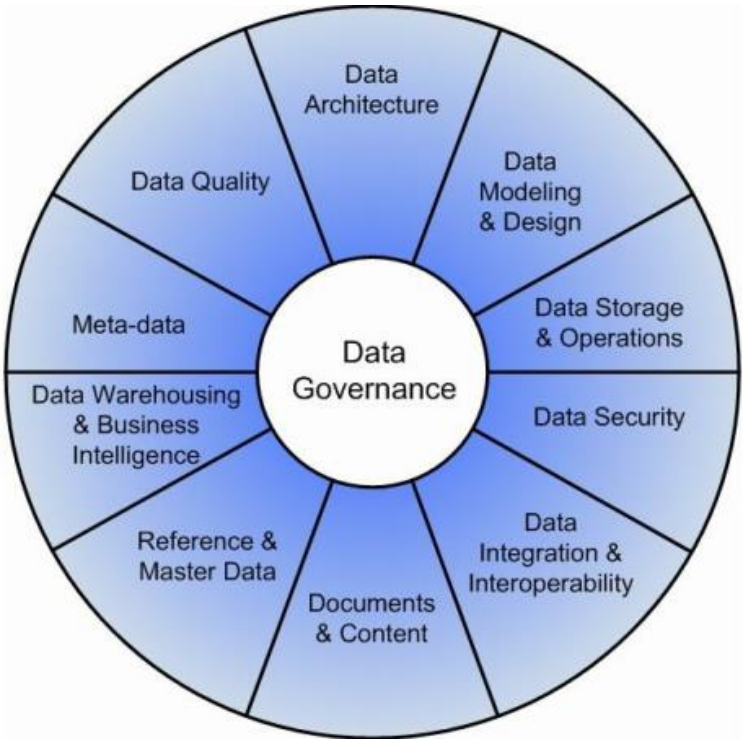
Um último tópico importante são os novos níveis de transparência, comunicação e conformidade, impostos pela LGPD. As empresas precisam ter uma comunicação transparente e assertiva para esclarecer os objetivos, os métodos e as bases legais utilizados no tratamento dos dados pessoais. Para atuar como canal de comunicação entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), as organizações também devem nomear um responsável pela governança interna de dados.

3. Governança de dados

Governança de dados é o exercício da autoridade e controle (planejamento, monitoramento e execução) sobre o gerenciamento de dados (REGO, 2013). Trata-se de um conjunto de premissas para gerenciar informações de uma empresa. Os principais objetivos para as empresas estabelecerem uma boa governança de dados são: definir, aprovar e comunicar estratégias, políticas e métodos sobre ativos de dados; garantir a conformidade; acompanhar e supervisionar a entrega de projetos e serviços de gerenciamento de dados; detectar e solucionar inconformidades relacionadas aos dados.

De acordo com o guia sobre conhecimento da gestão de dados, guia do Data Management Association (DAMA INTERNATIONAL, 2012), a governança de dados é a função central para orientar a execução das demais funções de dados, conforme modelo exposto na figura 2.

Figura 2 – Modelo de governança de dados DAMA DMBOK2



Fonte: DAMA International, 2014.

Com a leitura da figura acima, pode-se deduzir que governar dados é definir práticas e políticas de segurança, acesso, integração e monitoramento dos dados dentro das empresas. A governança de dados abrange diferentes características relacionadas às informações que coexistem e formam os dados. Esse controle se dá em aspectos dos dados, como: a arquitetura, modelagem e design de dados; armazenamento, físico ou virtual, integração e operações relacionadas; a segurança das informações e conteúdo de documentos; referências de dados e metadados; inteligência empresarial e qualidade de dados.

Na prática, governança de dados atua como uma entidade articuladora, que gere dados da organização, identifica riscos, e define políticas, atribuições e responsabilidades; através de oportunidades de melhoria e monitoramento da execução de ações e estratégias que visam o aprimoramento da maturidade no uso de dados.

Mesmo com a crescente transformação tecnológica, é perceptível nas empresas, a grande necessidade de utilização de documentos com a finalidade de mostrar os resultados de um determinado projeto. O Gerenciamento da documentação e conteúdo tem como objetivo de planejar, implementar e controlar atividades para armazenar, proteger e acessar dados encontrados em arquivos eletrônicos e registros físicos (texto, gráficos, imagens, áudio e vídeo), ou seja, o foco em dados não estruturados, não armazenados em sistemas relacionais (DAMA INTERNATIONAL, 2012). Com o excesso de documentos físicos, além do custo da impressão desnecessária, este documento, muita das vezes, não é armazenado em local seguro.

Com a chegada da LGPD, as organizações devem fazer um diagnóstico em torno de suas informações, seguido por uma análise detalhada acerca de quais práticas devem ser incluídas, mantidas ou modificadas, para assegurar a sua conformidade regulatória. Nos subitens a seguir, são apresentadas algumas etapas e responsabilidades relacionadas à governança de dados que deverão ser alteradas ou inseridas para execução desse controle em acordo com a nova legislação.

3.1 Conscientização de colaboradores

Para a adequação de empresas às definições da LGPD é importante que as organizações tenham plena conscientização sobre a lei; esta deve partir de iniciativa da própria da companhia, e pode gerar necessidades específicas que demandem terceirização do serviço, criação de departamentos específicos ou habilitação de seus profissionais para estas competências. A construção de uma cultura de privacidade e a conscientização de todos para a proteção de dados é essencial para a sustentabilidade do programa e o desenvolvimento de conceitos essenciais, como o *privacy by design* (privacidade desde a concepção). Um procedimento no qual a proteção de dados é planejada desde a concepção do projeto, em que leva-se em consideração possíveis obstáculos e soluções de mitigação desses riscos.

Segundo a ISO/IEC 27701:2019, controle 8.2.2 - Rótulos e tratamento da informação, convém que a organização assegure que as pessoas sob o seu controle estejam conscientes da definição de dados pessoais e saibam como reconhecer uma informação que é dado pessoal. Cada colaborador deverá estar ciente sobre o impacto da nova lei em sua atividade diária, consequentemente surge a necessidade de engajamento e orientação dos colaboradores em relação às vantagens dos requisitos da LGPD. Neste sentido, treinamentos sobre a lei são necessários para que se abram canais de discussão e esclarecimentos, capazes de treinar e qualificar os empregados da organização. É importante ainda, que os empregados saibam a quem, ou a que canais, recorrer em caso de dúvidas.

Com a implementação da LGPD nas rotinas, o profissional deverá ser capaz de ajustar-se às mudanças em suas atividades diárias: identificar todos os dados pessoais utilizados em seus processos, bem como quais procedimentos precisam ser adaptados à nova legislação.

3.2 Encarregado de proteção de dados

Para alguns segmentos, conforme regulamentado pela Autoridade Nacional de Proteção de Dados (ANPD), o encarregado de proteção de dados, é também conhecido como DPO - *Data Protection Officer* (ou Encarregado pela Proteção de Dados, em tradução livre para português). Este profissional será a pessoa responsável

na empresa por acompanhar todas as solicitações que dizem respeito à proteção dos dados pessoais, ou seja, o ponto focal facilitador da comunicação entre a organização, os titulares desses dados e a ANPD.

Com base nas melhores práticas e nos conceitos inspirados na GDPR, sugere-se que o DPO tenha conhecimento e perfil multidisciplinar, podendo opinar sobre diversos assuntos relacionados a questões técnicas e jurídicas, reportando-se diretamente à alta direção com devida imparcialidade.

Dentre as principais funções do DPO, destacam-se: informar e orientar sobre as obrigações e boas práticas a serem seguidas para adequação à legislação vigente; realizar o monitoramento do cumprimento da LGPD nas atividades de tratamento de dados da empresa, através de reporte de eventuais incidentes; ser intermediário na comunicação da empresa com a ANPD e com o titular dos dados. Suas atividades podem compreender: o auxílio durante fiscalizações; o apontamento de providências; o recebimento de demandas e reclamações; e esclarecimento de dúvidas em geral.

Entretanto é importante ressaltar que o encarregado não possui poderes determinantes, ele está habilitado a orientar, indicar e recomendar procedimentos, porém a decisão quanto à adoção ou não de suas instruções cabe à empresa. A responsabilidade decorrente de qualquer infração à LGPD será da empresa, exceto em casos específicos que não serão abordados neste estudo, como por exemplo, quando é provado que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. Segundo o Presidente do guia DAMA Brasil, Bergson L. Rego, as empresas que acreditam que o "DPO é uma espécie de "super-herói", capaz de assumir e resolver todos os problemas [...] já desperdiçaram recursos e a probabilidade da governança de dados gerar algum retorno para a organização é muito baixa" (REGO, 2019).

3.3 Mapeamento dos dados

O mapeamento dos dados pessoais é uma das fases mais importantes do processo de adequação de uma organização para as regras da LGPD. É a realização de um estudo completo dos dados pessoais tratados pela empresa como um todo, e onde a organização consegue mensurar a quantidade e o nível de complexidade dos dados e processos. Ela requer realizar um levantamento da empresa, identificando

quais dados pessoais estão sendo coletados, quais as áreas da empresa que realizam o tratamento, por quanto tempo e onde esses dados ficam armazenados, com quem são compartilhados e qual a finalidade do tratamento. Esta etapa deve ser executada detalhadamente e com bastante cuidado, pois poderá impactar nos passos futuros para adequação à lei.

Ao iniciar-se o mapeamento dos dados pessoais de uma empresa, deve-se realizar o estudo na estrutura organizacional da companhia, identificando as principais áreas que podem ser mais impactadas, pois possuem algum tipo de dado pessoal. Apesar disso, sugere-se que o mapeamento deva abranger todos os departamentos da companhia, pois pode haver algum dado pessoal transitando pelas áreas da organização. Todavia, a depender da escolha da empresa, poderão ser utilizados softwares e tecnologias para ajudar no suporte dessa fase.

Após o mapeamento dos dados, as organizações se tornam capazes de visualizar melhor seus fluxos e entender a dinâmica cíclica dos dados pessoais. Durante a realização do mapeamento muitas disparidades já podem ser identificadas e sinalizadas com as respectivas medidas para saná-las.

O mapeamento não é apenas uma necessidade para possibilitar a implantação do programa de adequação à LGPD, mas também uma exigência de vários artigos da lei que mencionam, expressamente, a necessidade de registro dos tratamentos de dados realizados por uma companhia. Além disso, mapear corretamente os dados tratados por uma empresa, rastreando todo o percurso do dado pessoal, desde a coleta até a eliminação, possibilitará uma melhor avaliação da segurança dos dados e a implementação correta de medidas de segurança que reduzam o potencial de eventuais incidentes.

3.4 Compartilhamento de dados com terceiros

A definição de uso compartilhado de dados pessoais, segundo a lei, refere-se à comunicação, difusão, transferência internacional e interconexão de dados pessoais. Segundo a ISO/IEC 27701:2019, anexo A.7.5 - Compartilhamento, transferência e divulgação de DP, a organização deve especificar e documentar os países e as organizações internacionais para os quais dados pessoais possam possivelmente ser transferidos. Também entra nessa lista o tratamento compartilhado

de bancos de dados pessoais por órgãos públicos que estejam cumprindo competências legais, ou entre esses e entidades privadas. Nesses casos, todas as partes envolvidas devem ter autorizações para executar o tratamento. Outros conceitos importantes definidos na lei são os dois principais agentes de tratamento de dados: o controlador, pessoa física ou jurídica que decide como e com qual finalidade os dados serão tratados; e o operador, pessoa física ou jurídica que realiza o tratamento em nome do controlador (BRASIL, 2018).

Ao compartilhar os dados pessoais com empresas terceiras, a depender da situação, os controladores que estiverem diretamente envolvidos são solidariamente responsáveis por qualquer dano causado, salvo nos casos previstos no artigo 43 da LGPD. A indenização ao titular dos dados também poderá ser responsabilidade do operador, uma vez que seja provado que ele não adotou as medidas de segurança necessárias, descumpriu as obrigações da legislação ou não seguiu as instruções lícitas do controlador.

Caso o controlador precise realizar o compartilhamento dos dados pessoais com terceiros, é de suma importância obter consentimento expresso do titular para esse fim, exceto em situações já previstas em lei que dispensam tal autorização, como por exemplo quando os dados já foram tornados públicos pelo titular. E ainda assim, os proprietários dos dados poderão acionar diretamente a organização para fins de reparação de danos sofridos, independentemente de ter sido uma falha da empresa terceira.

Segundo a ISO/IEC 27701:2019, controle 14.1.2 - Serviços de aplicação seguros em redes públicas, convém que a organização assegure que os dados pessoais transmitidos por redes de transmissão de dados não confiáveis estejam criptografados para a transmissão, e ainda enfatiza que a organização deve determinar e manter de forma segura os registros necessários ao suporte às suas obrigações para o tratamento do dado pessoal.

3.5 Relatório de impacto à proteção de dados

Sob o nome de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), a LGPD importou uma metodologia amplamente adotada pela legislação europeia, chamada Data Protection Impact Assessment (DPIA). Ela consiste em 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 de risco” (BRASIL, 2018).

Esse relatório apoia o princípio de responsabilidade e prestação de contas da LGPD, ajudando as organizações a provar que tomaram medidas técnicas e organizacionais apropriadas, conforme necessário. A falha em condução adequada do relatório, quando obrigatório, constitui uma violação da lei e poderá resultar em multas administrativas.

Tanto a LGPD quanto a GDPR não possuem uma definição da estrutura do relatório de impacto, permitindo que as organizações usem uma que complemente suas práticas de trabalho existentes. No entanto, seja qual for a metodologia utilizada, o RIPD ou DPIA normalmente consistirá nas seguintes etapas: identificação da necessidade; descrição do fluxo de informações; descrição da natureza, escopo, contexto e propósitos do processamento; identificação dos riscos para os direitos e liberdades dos titulares de dados; identificação de soluções para reduzir ou eliminar esses riscos; e integração das soluções no projeto (LOPES, 2019). Portanto, antes de realizar o relatório de impacto, é necessário catalogar todo o tipo de tratamento de dados que a empresa realiza, e verificar quais podem trazer risco aos titulares de dados.

3.6 Gestão de incidentes

De acordo com o artigo 48 da LGPD, torna-se um dever de um controlador comunicar a autoridade nacional e ao titular qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A organização deve estar preparada para o tratamento e resposta aos incidentes de segurança da informação (SI), e entender como será o processo de contingenciamento perante a situação, quem são os responsáveis pela não-conformidade, e como devem atuar os empregados e demais colaboradores. Nesta conjuntura, entende-se como incidente de SI qualquer ocorrência acidental ou ilícita relacionada à segurança dos dados; incluindo o acesso indevido e a perda ou apagamento de dados sem a intenção.

Com o avanço da tecnologia, aumento do conhecimento e a sofisticação cada

vez maior das invasões, as empresas precisam ter recursos de detecção e resposta a incidentes mais avançados. Ter uma equipe de resposta a incidentes focada na investigação de ameaças coletando mais informações (com a aprovação dos titulares), determinando vulnerabilidades e entendendo o que mais pode ter sido baixado ou se a ameaça original sofreu uma mutação e se espalhou. Fazendo uma análise completa para determinar a causa raiz e o possível impacto.

Neste sentido, também pode ser utilizado como parâmetro o conceito de "violação de dados pessoais" do Regulamento Europeu nº 679/2016 (GDPR) que consiste em evento acidental ou ilícito, que ocasione a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. Segundo o executivo da Embratel, Yanis Stoyannis, quando a segurança da informação é automatizada, o valor do custo de um vazamento de dados diminui expressivamente.

> Isso acontece porque você tem uma agilidade para identificar aquele problema, saber onde está tendo o vazamento, como conter aquilo e também notificar de forma precisa os seus clientes e a [futura] Autoridade Nacional. Significa mostrar para o mercado que você está efetivamente trazendo transparência e tratando os dados da melhor maneira possível (MUNDO MAIS TECH, 2019).

Dependendo da gravidade do incidente, e caso seja necessário para proteção dos titulares, a ANPD poderá determinar medidas compulsórias para reverter os prejuízos e a ampla divulgação dos incidentes em meios de comunicação. A LGPD também determina critérios para avaliação da gravidade do incidente, dentre eles a adequação das medidas técnicas adotadas para que os dados sejam criptografados para acesso por terceiros não autorizados. De acordo com a mesma lei, no artigo 50 é mencionado que um programa de governança em privacidade deve contar, no mínimo, com um plano de resposta a incidentes.

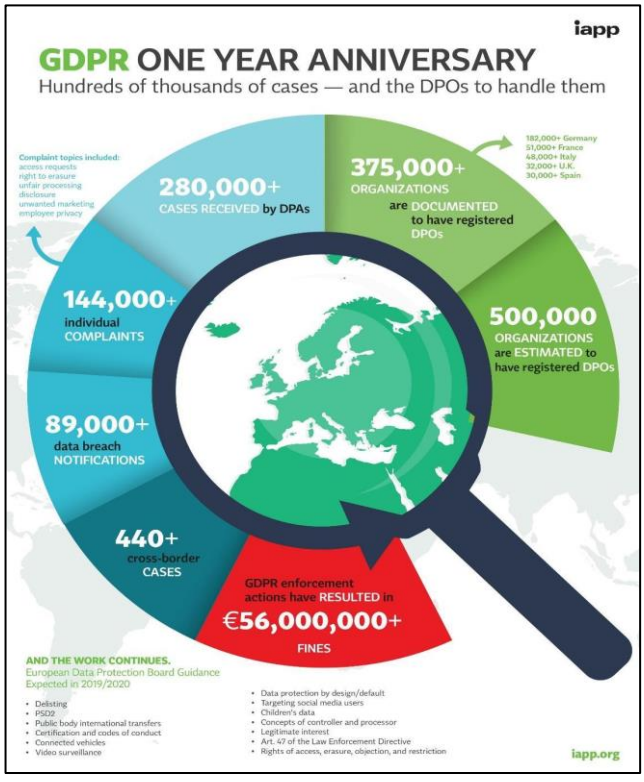
A equipe de resposta a incidentes investiga as ameaças em questão, coletando mais informações, determinando vulnerabilidades e entendendo o que mais pode ter sido baixado ou se a ameaça original sofreu uma mutação e se espalhou. Uma análise completa é feita para determinar a causa raiz e o possível impacto, além de gerar relatórios sobre o incidente para evitar futuros ataques e com esse estudo saberá como reagir e remediar o ataque e, em alguns casos, ferramentas para ajudar na remediação.

Diante da relevância do assunto é possível concluir que três principais tópicos estão relacionados a uma abordagem correta de incidentes de segurança: a elaboração prévia de um plano de resposta a incidentes; a devida comunicação à autoridade nacional e titulares; e a aplicação de medidas que reduzam riscos ou danos causados.

3.7 Casos reais de vazamentos de dados

Em 25 de maio de 2019, a GDPR completou um ano e uma das maiores associações de privacidade do mundo, a International Association of Privacy Professionals (IAPP) - em português, Associação Internacional de Profissionais de Privacidade - realizou um estudo sobre os impactos da aplicação da lei europeia, conforme mostrado na figura 3. De acordo com o IAPP, foram registrados mais de 89 mil casos de vazamento de dados, com um montante de multas superior a €56 milhões. Além disso, 440 casos envolveram violações em mais de um país e as autoridades de dados espalhadas pela Europa receberam mais de 280 mil casos por alguma infração contra as normas da GDPR (IAPP, 2019).

Figura 3 - Gráfico do estudo de aniversário da GDPR



Fonte: iapp.org, 2019.

No Brasil, alguns casos emblemáticos sobre incidentes de segurança podem servir de parâmetro sobre procedimentos a serem realizados, ou evitados, com relação aos incidentes de segurança. Como foi o caso do escândalo de dados do Facebook, que veio à tona no final de 2018 e afetou mais de 400 mil brasileiros. “Por anos, o Facebook ofereceu a algumas das maiores empresas mundiais de tecnologia acesso mais intrusivo aos dados pessoais de seus usuários” (THE NEW YORK TIMES, 2018). Cabe ressaltar que, em caso de incidentes, vazamento ou uso indevido dos dados pessoais, as empresas que possuem a tutela dos dados devem seguir plano de contingência e mitigação dos danos, além da comunicação aos titulares e à ANPD.

Os principais fatores que desencadeiam os incidentes e trazem risco quanto à segurança da informação, podem ser resumidos em dois aspectos: falha humana, geralmente pela falta de treinamento; ou tecnologia, no qual empresas e consumidores dependem cada vez mais de uma complexidade maior de algoritmos e de sistemas.

Segundo comentou Yanis Stoyannis, no seminário organizado pelo jornal Valor Econômico, “a tecnologia está em todos os ramos e segmentos da sociedade, sendo cada vez mais adotada. É a expansão da internet, IoT, Inteligência Artificial, Machine Learning, entre outras. Mas quando a gente fala de tecnologia a gente fala de software” (MUNDO MAIS TECH, 2019). Ou seja, tecnologias são desenvolvidas e podem sofrer ataques de vulnerabilidades e conter falhas. Yanis Stoyannis, também sugeriu que a empresa se questione internamente: “quanto custa uma violação de dados e quanto custa investir na adequação?”. Obtendo a devida resposta, a empresa conseguirá se organizar e se blindar de possíveis ataques (MUNDO MAIS TECH, 2019).

Apesar da LGPD não estar em vigor e a ANPD ainda não ter sido criada, o Ministério Público do Distrito Federal e Territórios (MPDFT) trabalha nos casos de vazamentos de dados no país. As investigações sobre os casos descritos abaixo foram conduzidas por este órgão público recentemente.

Em setembro de 2019, o MPDFT identificou o vazamento de dados cadastrais no Banco Pan, uma vulnerabilidade no armazenamento de dados em nuvem que continham aproximadamente um milhão e duzentos mil arquivos relacionados à

dados pessoais. De acordo com o site do próprio órgão: “o MPDFT aponta que uma provável vulnerabilidade na ferramenta de armazenamento de dados em nuvem [...] expôs indevidamente 245 gigabytes, o que corresponde a 1.235.151 arquivos de documentos relacionados a clientes do Banco” (MPDFT, 2019).

Outro caso que teve vasta repercussão foi o da Unimed. Uma falha grave de segurança expos dados pessoais de clientes, como nome completo, CPF, nome da mãe, código beneficiário, e-mail e dados de dependentes, bem como acessos a logins médicos, e-mails internos, imagens de problemas internos de centros de saúde, planilhas financeiras. Também ocorreu vazamento de dados sensíveis, como exames de pacientes, certidões de óbito e imagens de raio X. Segundo o grupo WhiteHat Brasil, empresa que realizou a denúncia do incidente ao site Olhar Digital, “o vazamento de dados possivelmente está afetando diversos sistemas da operadora. Por enquanto, o número de pessoas afetadas é incerto, mas pode chegar à casa dos milhões” (OLHAR DIGITAL, 2019).

Nestes casos, uma medida prévia que mitiga riscos causados pelo vazamento de dados é a encriptação de dados pessoais. Isto porque, dados vazados que estejam encriptados não podem ser facilmente traduzidos por indivíduos que não tem acesso a respectiva chave de desencriptação. Entretanto, apesar de ferramentas de encriptação serem facilmente encontradas no mercado, a maioria das empresas ainda não implementa essa medida de segurança.

4. Segurança de dados

A Lei Geral de Proteção de Dados prevê que as empresas adotem boas práticas de Segurança da Informação e de Governança dos dados como fator determinante. Importante enfatizar que um dos aspectos principais da Governança é a responsabilidade de garantir a integridade e segurança dos dados de uma organização.

4.1 Importância para organizações

Como é descrito na norma ISO/IEC 27002 (2005) - que foca nas boas práticas para a gestão da segurança da informação - “é um ativo que, como qualquer outro ativo importante para os negócios consequentemente necessita ser adequadamente protegida”, ou seja, a informação é tudo aquilo que tem importância para a organização, é o ativo de maior valor dentro dela, e por esse motivo faz jus à proteção.

A segurança da informação fornece proteção aos dados e impede o acesso às informações por quem não tem permissão, a fim de garantir a confidencialidade exigida. Garante também a integridade e disponibilidade dos dados, para que não haja qualquer modificação nos dados ou obstrução de acesso a profissionais autorizados. Surge então a necessidade de criação de diretrizes que orientem como compreender e tratar a segurança da informação dentro das organizações.

Em relação a esse cenário, informado no fórum de auditoria, que foi publicada em 06 de agosto de 2019, a ISO 27701, baseada na ABNT NBR ISO/IEC 27001:2013 e na ABNT NBR ISO/IEC 27002:2013, e estende os seus requisitos e diretrizes para considerar, em complementação à segurança da informação, a proteção da privacidade dos titulares de dados pessoais. A norma estabelece os requisitos e orientações para implantação e manutenção sistema de gerenciamento da privacidade da informação, complementando e integrando (ou estendendo) os

objetivos e controles da já conhecida ISO 27001, ou seja, a ISO 27001 apoiada com a ISO 27701, irá aumentar o nível de controle para as organizações.

Muitas empresas formulam regras de SI utilizando como base a norma ISO/IEC 27001, cuja última versão de 2013, estabelece as melhores práticas para implementação de um Sistema de Gestão de Segurança da Informação. De acordo com essa norma, a administração da própria empresa deve elaborar uma política de SI adequada ao propósito da organização e necessidades do negócio, que garanta o comprometimento da companhia com a aplicação dos requisitos e com melhoria contínua do Sistema de Gerenciamento da Segurança da Informação gerado. Esse conjunto de regras deve ser um documento divulgado dentro da organização, além de estar acessível para todas as partes interessadas.

A ISO/IEC 27001: 2013 é a maneira mais eficiente de mitigação do risco de sofrer uma violação de informações de dados (SKYPRO, 2018). A ISO foi projetada para identificar, gerenciar e reduzir o ramo de ameaças às quais suas informações são sujeitas regularmente. Por isso, as empresas precisam apresentar uma certificação ISO / IEC 27001: 2013 para expansão dos seus negócios, garantindo um gerenciamento assertivo nos ativos de informação.

Na figura 4, são apresentados os principais pilares que compõem a ISO/IEC 27001. Sendo eles: Organização Interna, Dispositivos móveis e trabalhos remotos, Segurança em RH, Gestão de Ativos, Tratamento de Mídias, Controle de Acesso (físico e sistema), Criptografia, Segurança Física, Equipamentos, Segurança nas Operações, Proteção contra malware, Cópias de segurança, Controle de software operacional, Gestão de vulnerabilidade, Segurança de dados, Transferência da informação, Segurança em desenvolvimento e suporte, Segurança na informação da cadeia de suprimentos, Gestão de incidentes, Requisitos Legais.

Figura 4 - Pilares da ISO 27001

Fonte: Website Skypro[2]

Tendo uma análise mais profunda sobre esses aspectos, entende-se que a segurança da informação busca através de um conjunto de controles adequados, estabelecidos e implementados, garantir a restrição do acesso de pessoas não autorizadas, consistência e disponibilidade das informações guardadas.

O sistema de gestão de segurança da informação é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação (FERREIRA; ARAUJO, 2008).

Como diretriz adicional, a ISO/IEC 27701, controle 5.1.1 - Políticas para segurança da informação, informa que a organização deve produzir uma declaração quanto ao apoio e comprometimento para alcançar *compliance* com as regulamentações e legislações de proteção de dados pessoais aplicáveis, e com termos contratuais acordados entre a organização e seus parceiros, subcontratados e seus terceiros aplicáveis (clientes, fornecedores, etc), para os quais convém que se especifiquem claramente as responsabilidades entre eles.

[2] Disponível em < https://skypro.co.id/iso-27001/>. Acesso em: 01 dez. 2019.

4.2 Política de Segurança da Informação

A elaboração de uma política de Segurança da Informação (SI) é uma ferramenta para garantir que a organização fique dentro das normas. Com ela, é possível que o ambiente de tecnologia da informação seja seguro, através de uma mudança cultural a ser implantada dentro da organização. A política deve ser construída pela própria organização de forma que mais se adeque às suas necessidades do negócio em relação à SI. Abaixo são retratados os principais tópicos de uma política de SI:

- Segurança física e lógica:

Estabelecer uma política de controle de acesso ao ambiente computacional - no contexto de *need to know*, onde somente pessoas autorizadas possuem acesso mínimo necessário ao desempenho das funções - determinando uma inclusão e revogação desses acessos quando necessários. Caso seja necessária a presença de algum funcionário terceiro, por suas instalações utilizadas para os serviços prestados à organização, deve adotar proteções passivas e, quando possível, separar fisicamente as instalações utilizadas pelos operadores das instalações de uso da empresa possivelmente presentes no local.

- Classificação e tratamento das informações:

Faz-se necessário definir uma diretriz em relação a classificação e tratamento das informações, pois constarão os níveis de classificação da informação correlacionada a Lei Geral de Proteção de Dados. Isso inclui uma diretriz sobre o tratamento dos dados, contendo orientações sobre o que são dados pessoais e sensíveis e a devida forma de coleta, armazenamento, processamento e exclusão destas informações prevendo a definição do DPO e o detalhamento de suas atribuições.

> Antes de se iniciar o processo de classificação, é necessário conhecer o processo de negócio da organização, compreender as atividades realizadas e, a partir disso, iniciar as respectivas classificações. As informações podem ser classificadas em informações públicas, quando não necessita de sigilo algum; informações internas, quando o acesso externo às informações deve, ser negado; e informações confidenciais, as informações devem ser confidenciais dentro da empresa e protegida contra tentativas de acesso externo. (FERREIRA; ARAUJO, 2008).

De acordo com a LGPD, a organização que trata dados pessoais sensíveis ou de crianças e adolescentes deve conscientizar seus colaboradores sobre a necessidade de cuidados específicos quando do tratamento destes dados pessoais. Segundo a ISO/IEC 27701:2019, controle 7.2.1 - Identificação e documentação do propósito, convém que a organização identifique e documente os propósitos específicos pelos quais os dados pessoais serão tratados.

- Confidencialidade das Informações:

Segundo a ISO/IEC 27701:2019, na implementação do controle 13.2.4, devem ser criados acordos de confidencialidade e não divulgação, ou seja, convém que a organização assegure que os indivíduos que operam sob seu controle com acesso aos dados pessoais estejam sujeitos a um acordo obrigatório de confidencialidade.

Outro ponto importante é sobre o acesso as estações de trabalho que deve ser feito através de credenciais de acesso individual, composto por combinação de uma credencial de identificação (UserID) e uma credencial de autenticação (senha / PIN). Todos os usuários devem receber credenciais de acesso individuais, contendo um UserID e uma senha, que deverá ser composta por pelo menos 8 caracteres (pelo menos 1 caractere numérico, pelo menos 1 caractere alfabético, pelo menos 1 caractere especial, não pode conter 3 ou mais caracteres idênticos consecutivos) e os UserIDs de um usuário não devem ser atribuídos novamente a outros usuários, mesmo em momentos diferentes. A empresa deverá ter completa rastreabilidade de acesso realizados nas informações da sua organização, a fim de identificar origem, autor, data/hora e informação acessada.

As informações envolvidas em transações On-line devem ser protegidas contra falhas na transmissão, rotas indevidas, alteração, duplicação, reenvio e exposição não autorizadas.

- Serviço de e-mail:

Faz-se necessário um documento que oriente e regule o modo de utilização do e-mail corporativo, que deverá ser utilizado exclusivamente para o desempenho da atividade de trabalho decorrente das obrigações contratuais, observadas as obrigações legais vigentes e de acordo com as seguintes regras comportamentais.

- Incidentes de Segurança:

Segundo a ABNT NBR ISO/IEC 27701:2019, para implementação do controle 16.1.1 - Responsabilidades e procedimentos, como parte do processo de gestão de incidentes de segurança da informação global, convém que a organização estabeleça responsabilidades e procedimentos para a identificação e registro de violações de dados pessoais. Ou seja, no caso de avarias ou incidentes nos seus sistemas de informação, devem ser adotados procedimentos operacionais específicos para a execução das atividades de restauração. As empresas também devem possuir também uma diretriz para o tratamento e resposta à incidentes de Segurança da Informação de como será o processo de contingenciamento em caso de um incidente de SI, atribuindo responsabilidade a pessoas específicas que respondem aos incidentes e como devem atuar os empregados e demais colaboradores diante de um incidente de SI.

- Proteção contra códigos maliciosos:

Estabelecer uma diretriz acerca de proteções contra malware, ou seja, código malicioso destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, prevendo medidas a serem adotadas para evitar ameaças.

- Backup:

O backup é um requerimento de negócio que possibilita a recuperação dos dados e aplicações em caso de eventos tais como desastres naturais, falhas em sistema de disco, sabotagem, erro de entrada de dados, falha de sistema operacional, falha humana e solicitações jurídicas, com o objetivo de manter a integridade e disponibilidade da informação e dos recursos de processamento. Possuir controle que garanta a verificação da integridade das informações na geração e na restauração da cópia de segurança, gerando um alerta caso ocorra alguma falha.

A documentação dos procedimentos de backup do sistema deve especificar as instruções necessárias, para execução de cada tarefa relacionada ao backup. A estipulação de premissas de backup, com o objetivo de proteger as informações armazenadas em meio digital, realizando o monitoramento de ativos e dos serviços da informação para normatizar como se dará o acompanhamento do cumprimento das determinações. “É evidente que o procedimento de backup é um dos recursos

mais efetivos para assegurar a continuidade das operações em caso de paralisação na ocorrência de um sinistro" (FERREIRA; ARAUJO, 2008, p. 133).

- Descarte:

Segundo a ABNT NBR ISO/IEC 27701:2019, como diretriz de implementação em 8.4.2 - Retorno, transferência ou descarte de DP, em algum momento, os dados pessoais podem precisar ser descartados de alguma maneira. Isto pode envolver o retorno dos dados pessoais para o cliente, a transferência deles para outra organização ou para um controlador de dados pessoais (por exemplo, como um resultado de uma fusão), exclusão ou outra forma de destruição deles, desanonimização ou o seu arquivamento. É bastante importante que a capacidade para o retorno, transferência e/ou descarte dos dados pessoais sejam gerenciados de forma segura.

4.3 Papeis e responsabilidades

A Lei Geral de Proteção de Dados ainda não detalha quais serão os controles exigidos para que a proteção e privacidade sejam alcançadas, deixando para a ANPD – Agência Nacional de Proteção de Dados – essa possibilidade. Em seu artigo 46, a LGPD descreve o seguinte:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

As boas práticas deverão fazer parte da rotina dos empregados, dos prestadores de serviço e quaisquer outras pessoas que tratem dados afim de evitar o acesso não autorizado de dados, situações acidentais ou ilícitos de destruição. Percebe-se que a lei não exclui a responsabilidade do agente nesses casos, pelo contrário o coloca como ator na prevenção de tais incidentes, sendo sua obrigação adotar as medidas previstas (TEIXEIRA; ARMELIN, 2019).

O dado, desde a sua coleta, poderá percorrer diversas fases de tratamento, sendo que de acordo com o Princípio da Segurança, em qualquer delas, tanto o agente de tratamento, como também, qualquer pessoa que, possa vir a intervir numa dessas fases estão obrigados a garantir a segurança em relação aos dados pessoais,

mesmo após o término do seu tratamento (TEIXEIRA; ARMELIN, 2019).

Importante destacar que a adoção de uma política de segurança de informação como uma norma de cumprimento obrigatório deve ser tratada como tal, no sentido de que aquele que descumprir os procedimentos deve submeter-se às sanções nela previstas. A abordagem precisa ser firme, para adequação dos desvios de conduta das pessoas que têm acesso às informações da organização não devem ser tolerados aplicando medidas cabíveis, caso necessário. A realização de uma revisão periódica da política se faz necessária para que sempre reflita da melhor forma possível a realidade informacional da organização.

Segundo Matthieu Grall, da *Nationale de l'Informatique et des Libertés*, pesquisador independente para a proteção de dados pessoais:

> Apesar dos riscos de não cumprir essas regulamentações, muitas organizações simplesmente não estão prontas e precisam de orientação. Com o número de reclamações e multas relacionadas à privacidade e à proteção de dados em alta, a necessidade desse padrão agora é óbvia (CBN RECIFE, 2019).

Enfim, as empresas devem estar conscientes da preservação de suas informações, ter uma gestão estruturada e um excelente tratamento e resposta aos incidentes que possam ocorrer. Portanto, proteger as informações da organização faz parte do processo e sempre será primordial para adequação a Lei Geral de Proteção de Dados.

5. Conclusão

5.1 Considerações finais e contribuições da pesquisa

Legislações voltadas à proteção de dados pessoais ainda estão muito recentes no Brasil. Apesar do que o senso comum sugere, a LGPD não foi criada para diminuir ou proibir negócios, mas para criar oportunidades para que empresas ganhem confiança dos clientes através da segurança de dados. A estratégia para fortalecer o mercado se depara com as diretrizes trazidas pela lei para processamento de dados pessoais, que geram desafios operacionais e demandam investimento de recursos e tempo.

As empresas terão que passar por mudanças relevantes em seus ambientes de tecnologia da informação (LGPD BRASIL, 2019). O primeiro passo é iniciar o processo de *Due Diligence* sobre dados pessoais, ou seja, identificar os dados pessoais, sensíveis, públicos, anonimizados, e de crianças e adolescentes, que a empresa possui em seu domínio. Em seguida, verificar quais departamentos, operadores, meios físicos e digitais estão permeando esses dados. Com isso é possível mensurar o nível de exposição da empresa à lei.

Igualmente importante à etapa de identificação dos passos é a criação de regras boas práticas e de governança, que determinem normas de segurança e procedimentos de mitigação de riscos no tratamento de dados pessoais.

Em relação a tratamento de dados, as empresas devem ficar atentas às 20 atividades descritas no artigo 5º, Inciso X, entre elas: coleta, acesso, distribuição, armazenamento e eliminação. Todas elas devem estar aderentes aos princípios gerais descritos no artigo 6 da lei, através da criação e revisão de contratos, termos e políticas para uso interno e externo. Segundo a ISO/IEC 27701:2019, se deve assegurar que processos e sistemas sejam projetados de tal forma que a coleta e o tratamento (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado.

Gestão do consentimento e anonimização, e gestão dos pedidos dos titulares são dois procedimentos importantes perante a LGPD. Investir em controles de solicitações dos titulares e na criação de um banco de dados com todos os pedidos, são boas estratégias de negócio para que as empresas fortifiquem a confiança com os titulares dos dados.

Em atendimento às exigências da Autoridade Nacional de Proteção de Dados e de outros órgãos do Sistema Nacional de Proteção do Consumidor, é necessário que o controlador disponha do Relatório de Impacto para prestar contas sobre os processos de tratamento de dados. A condução indevida do relatório pode caracterizar-se como uma violação da lei e multas simples ou diárias podem ser aplicadas.

No ramo da Segurança de Dados a lei conduz à adoção de medidas para proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas. Qualquer incidente de segurança deve ser comunicado aos órgãos fiscalizadores e à imprensa, caso acarrete algum risco ou danos. Os padrões técnicos mínimos referido no § 1º do artigo 46 da LGPD deve incluir necessariamente a conformidade dos agentes de tratamento de dados à ISO 27001 estendida com a ISO 27701.

Apesar de precisarem se adaptar, as empresas brasileiras aparentam não estarem prontas para se adaptarem às novas regras de privacidade. Segundo Bergson L. Rego, presidente do DAMA Brasil, estar em conformidade com a lei ainda gera muitas dúvidas e muitas iniciativas se perdem no alinhamento de alguns princípios básicos. “Não existe a possibilidade de qualquer empresa estar totalmente aderente à LGPD sem um programa de governança de dados efetivo” (REGO, 2019).

Com este cenário, o deputado Carlos Bezerra protocolou no final de outubro de 2019 o Projeto de Lei nº 5.762/2019, que propõe prorrogar a data da entrada em vigor da LGPD para 15 de agosto de 2022. Para o parlamentar, faltando pouco mais de dez meses para a lei entrar em vigor, o número de empresas brasileiras que iniciaram o processo de adaptação ao novo cenário jurídico é muito pequeno.

> Isso é o que aponta o estudo Brazil IT Snapshot, da consultoria Logicalis, baseada em pesquisa realizada junto a 143 empresas nacionais, cujos resultados foram divulgados pelo jornal Valor na edição de 28 de setembro deste ano. De acordo com o estudo, apenas 17% das instituições consultadas dispõem de iniciativas concretas ou já implementadas em

> relação à matéria. Além disso, 24% tiveram contato com o tema somente por meio de apresentações, e apenas 24% "têm orçamento específico para colocar em prática ações que garantam a proteção de dados de acordo com as exigências legais". (MATO GROSSO, 2019).

Outra justificativa para postergar o prazo é a "morosidade" do Poder Público na instalação do órgão governamental ANPD. De acordo com o deputado, "ainda que a Autoridade seja instalada [...] decerto não haverá tempo hábil até agosto de 2020 para que todas as propostas de regulamentação sobre a matéria sejam discutidas pela sociedade e aprovadas pelo órgão" (MATO GROSSO, 2019).

Na análise de Patricia Peck, sócia do Pires & Gonçalves - Advogados Associados e especialista em Direito Digital, há vantagens e desvantagens na proposta. Do ponto de vista das instituições, há um ganho de tempo para se adequarem às diretrizes da lei. Entretanto, é necessário iniciar os ajustes nesse momento e não deixar postergar novamente. Por outro lado, a prorrogação da lei pode ter efeitos negativos para o país, pois no âmbito comercial pode haver barreiras junto à União Europeia e impacto nos investimentos internacionais (PINHEIRO, 2019).

A OABRJ emitiu uma nota técnica de repúdio ao Projeto de Lei 5.762/2019, pois o adiamento significa "flagrante violação de direitos fundamentais, trazendo consigo, ainda, nefasto efeito econômico, que diante do panorama interno, pode agravar ainda mais a crise que assola o nosso país" (BANDEIRA; SOUZA, 2019).

No início de dezembro de 2019, o projeto de lei estava em análise, aguardando parecer do Relator na Comissão de Constituição e Justiça e de Cidadania (CCJC)[3]. Caso seja aprovado, os impactos causados no Brasil podem ser explorados em trabalhos futuros.

5.2 Trabalhos futuros

Existem outros aspectos que impactam o ambiente corporativo que não foram abordados nesse estudo, e podem tornar-se alvo de trabalhos futuros, como a certificação por auditoria especializada em práticas relacionadas à LGPD, análise

[3] Informação extraída do site <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704> em 01 dec. 2019.

mais profunda sobre a validação do término do tratamento, prevenção de conflitos para mitigação do contencioso judicial (LGPD BRASIL, 2019).

Sugestões para trabalhos futuros envolvendo esta análise incluem o desenvolvimento de uma ferramenta que auxilie no processo de mapeamento dos dados e na realização de um estudo completo dos dados pessoais tratados pelo Centro de Ciências Exatas e Tecnologia. Também pode ser sugerido um estudo de caso de sucesso das empresas que prontamente se adequaram a Lei Geral de Proteção de Dados e os benefícios de adequação para o mercado.

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27701: Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Rio de Janeiro, 2019.

BANDEIRA, L.; SOUZA, M. OABRJ critica, em nota técnica, proposta de adiamento para vigência da Lei Geral de Proteção de Dados. Disponível em: <https://www.oabrj.org.br/noticias/oabrj-critica-nota-tecnica-proposta-adiamento-vigencia-lei-geral-protecao-dados>. Acesso em: 01 dez. 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018, institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 nov.2019.

CABRAL, C.; CAPRINO W. Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

CBN RECIFE. ISO publica primeiro padrão internacional sobre privacidade no gerenciamento de informações. Disponível em: <https://www.cbnrecife.com/movimentoeconomico/artigo/iso-publica-primeiro-

padrao-internacional-sobre-privacidade-no-gerenciamento-de-informacoes>. Acesso em: 29 nov. 2019.

CONSELHO DA JUSTIÇA FEDERAL. Regulação, efetividade e segurança jurídica dominam debates no último dia do seminário sobre a LGPD. Disponível em: <https://www.cjf.jus.br/cjf/noticias/2019/05-maio/regulacao-efetividade-e-seguranca-uridica-dominam-debates-no-ultimo-dia-do-seminario-sobre-a-lgpd>. Acesso em: 28 nov.2019.

DAMA INTERNATIONAL. The Dama Guide to the Data Management Body of Knowledge (Dama-Dmbok) Portuguese Edition, 2012.

ÉPOCA NEGÓCIOS ONLINE. 84% das empresas brasileiras não estão preparadas para a LGPD. Disponível em: <https://epocanegocios.globo.com/tecnologia/noticia/2019/11/84-das-empresas-brasileiras-nao-estao-preparadas-para-lgpd.html>. Acesso em: 24 nov. 2019.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018, p. 29.

EXAME. LGPD: Empresas estimam prazos de até um ano para adequação à lei. Disponível em: <https://exame.abril.com.br/negocios/economidia/lgpd-empresas-estimam-prazos-de-ate-um-ano-para-adequacao-a-lei/>. Acesso em: 29 nov. 2019.

FERREIRA, F.; ARAUJO, M. Política de segurança da informação: guia prático para elaboração e implementação. 2ª edição. Rio de Janeiro: Ciência Moderna, 2008.

GLAB PARA MICROSOFT. Lei geral de proteção de dados impacta seus negócios. Disponível em: <https://epocanegocios.globo.com/Publicidade/Microsoft/noticia/2019/05/lei-geral-de-protecao-de-dados-impacta-seus-negocios.html>. Acesso em: 28 nov. 2019.

GOMES, H. Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml>. Acesso em: 12 jun. 2019.

IAPP. *GDPR One Year Anniversary – Infographic*. Disponível em: <https://iapp.org/resources/article/gdpr-one-year-anniversary-infographic/>. Acesso em: 25 mai. 2019.

LGPD BRASIL. O que a empresa deve fazer. Disponível em: <https://www.lgpdbrasil.com.br/> Acesso em: 30 nov. 2019.

LOPES, P. RIPD e DPIA, o que são e quando usar. Disponível em: <https://periciacomputacional.com/ripd-e-dpia-o-que-sao-e-quando-usar/>. Acesso em: 20 out. 2019.

MATO GROSSO. Projeto de Lei 5.762/19, altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 15 de agosto de 2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704>. Acesso em: 01 dez. 2019.

MPDFT. MPDFT abre inquérito para investigar vazamento de dados de clientes do banco Pan. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/11209-mpdft-abre-inquerito-para-investigar-vazamento-de-dados-de-clientes-do-banco-pan >. Acesso em: 01 dez. 2019.

MUNDO MAIS TECH. Como a LGPD pode fomentar a inovação na sua empresa. Disponível em: <https://mundomaistech.com.br/2019/12/03/como-a-lgpd-pode-fomentar-a-inovacao-na-sua-empresa/>. Acesso em: 10 jan. 2020.

OLHAR DIGITAL. Falha grave de segurança expõe dados sensíveis de clientes da Unimed. Disponível em <https://olhardigital.com.br/noticia/-exclusivo-falha-grave-de-seguranca-expoe-dados-sensiveis-de-clientes-da-unimed/92979>. Acesso em: 01 dez. 2019.

PINHEIRO, P. LGPD: os prós e contras de prorrogar a lei para 2022. Disponível em: <https://www.pgadvogados.com.br/midia-insight/lgpd-os-pros-e-contras-de-prorrogar-a-lei-para-2022>. Acesso em: 01 dez. 2019.

POHLMANN, S. LGPD Ninja: Entendendo e implementando a Lei Geral de Proteção de Dados na Empresa. Rio de Janeiro: Fross, 2019.

REDAÇÃO JURIS CORRESPONDENTE. A GDPR (proteção de dados europeia) e o seu impacto no Brasil. Disponível em <https://blog.juriscorrespondente.com.br/gdpr-e-protecao-de-dados-tudo-o-que-voce-precisa-saber/>. Acesso em: 01 mar.2020.

REGO, B. A LGPD está impulsionando a adoção de programas de governança de dados. Disponível em: <https://www.itforum365.com.br/a-lgpd-esta-impulsionando-a-adocao-de-programas-de-governanca-de-dados/>. Acesso em 20 out. 2019.

REGO, B. Gestão e Governança de Dados: Promovendo dados como ativo de valor nas empresas, Rio de Janeiro: Brasport, 2013.

REINALDO FILHO, D. A Diretiva Europeia sobre Proteção de Dados Pessoais - uma Análise de seus Aspectos Gerais. Disponível em: <http://www.lex.com.br/Doutrinas.aspx>. Acesso em: 25 mai. 2019.

RULE J.; GREENLEAF G. *Global Privacy Protection: The First Generation*, Cheltenham, Northampton: Edward Elgar Pub, 2010, p. 83.

SISQUALIS. Principais Aspectos da Lei Geral de Proteção de Dados – LGPD. Disponível em: <https://sisqualis.com.br/principais-aspectos-da-lei-geral-de-protecao-de-dados-lgpd-2/>. Acesso em 25 mai. 2019.

SKYPRO. ISO 27001. Disponível em < https://skypro.co.id/iso-27001/>. Acesso em: 01 dez. 2019.

TANAKA, A. Aspectos jurídicos da implementação da Lei Geral de Proteção de Dados Pessoais. Trabalho de Conclusão de Curso de Direito. Rio de Janeiro: Universidade Estácio de Sá. 2019.

TEIXEIRA, T.; ARMELIN, R. Lei Geral de Proteção de Dados Pessoais – comentada artigo por artigo. São Paulo: Juspodivm, 2019.

THE NEW YORK TIMES. Facebook forneceu mais dados pessoais a gigantes da tecnologia do que o revelado. Disponível em: < https://www1.folha.uol.com.br/mercado/2018/12/facebook-forneceu-mais-dados-pessoais-a-gigantes-da-tecnologia-do-que-o-revelado.shtml>. Acesso em 01 mar. 2020.

WARREN S.; BRANDEIS L. *The Right to Privacy*. Disponível em: <https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents>. Acesso em: 30 nov. 2019.

GLOSSÁRIO

Glossário em ordem alfabética dos termos definidos no artigo 5º da LGPD[4].

Agentes de tratamento: o controlador e o operador.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Encarregado: 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).

[4] Link para o texto completo compilado no site do Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 06 fev. 2020.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

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.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.