Lei Geral de Proteção de Dados (LGPD) - Da Teoria a Prática

Rodolfo Barros
Francyelcyo Pussi Farias

RESUMO

O objetivo deste artigo é apresentar os principais elementos envolvidos na Lei Geral de Proteção de Dados (LGPD) de acordo com a Lei 13709, de 14 de agosto de 2018, qual a situação atual da Autoridade Nacional de Proteção de Dados (ANPD), como o mercado de trabalho tem abordado esse assunto no Brasil, os impactos da lei de proteção de dados pessoais Europeia (GDPR) e como as empresas no Brasil podem se preparar para se adequarem as novas exigências legais.

A metodologia utilizada para tratar da Governança da Segurança da Informação foi a PDCA (Plan, Do, Check, Act) embasada nas boas práticas de Governança estabelecidas na ISO 27001 e ISSO 27002.

É esperado que esse Artigo sirva como referência e ponto de partida para aqueles profissionais que estão com a responsabilidade de adotar medidas de segurança para garantir que sua empresa esteja em conformidade após a LGPD começar a vigorar.

Palavras-chave: Lei Geral de Proteção de Dados. LGPD. GDPR no Brasil. Privacidade. Proteção de Dados Pessoais.

1 **INTRODUÇÃO**

Desde agosto de 2018 quando a Lei Geral de Proteção de Dados nº 13709, mais conhecida como LGPD, foi aprovada no Congresso Nacional, empresas de diversos setores e de diversos portes tem se preocupado em entender qual a dimensão e os impactos que as medidas de segurança voltadas a proteção de dados pessoais e à privacidade trarão aos seus negócios. A princípio a data estabelecida para o início da vigência da LGPD era 14/08/2020, porém esse prazo foi postergado para 03/05/2021 através da MP 959 de 2020.

Muitas são as dúvidas e incertezas, principalmente de médias e pequenas empresas que não estão acostumadas a investir em governança de segurança da informação, que por ter um escopo muito abrangente e encontrar disponível no mercado diversas soluções, acaba se tornando um buraco sem fundo no que se refere a investimentos.

As grandes corporações apesar de já estarem habituadas a destinar uma parcela considerável de seu orçamento para adotar medidas de segurança, provavelmente estarão mais expostas e suscetíveis a altos níveis de fiscalizações, que poderão partir espontaneamente por decisão da Autoridade Nacional de Proteção de Dados (ANPD) ou por denúncias feitas por cidadãos e até mesmo concorrentes, que poderão exigir da ANPD que a empresa apresente evidências das medidas de segurança aplicadas em sua base de informação e dados pessoais.

Falando um pouco da ANPD, essa é uma grande incógnita uma vez que a poucos meses da LGPD começar a vigorar, ainda não foi encontra-se criado de fato esse agência, impossibilitando as empresas e profissionais da área a fazerem consultas, tirar dúvidas e até mesmo submeter para avaliação investimentos direcionados para atender as novas exigências para a proteção de dados pessoais. O que temos disponível até o momento é o que está descrito

no LGPD, ou seja, a nomeação do Conselho Diretor e sua composição, porém ainda não temos canais para contato e tão pouco acesso aos seus integrantes.

A movimentação que tem acontecido por parte dos profissionais envolvidos na implementação da LGPD nas empresas, está se baseada nas medidas adotas por empresas europeias, uma vez que a LGPD foi criada com base na GDPR (General Data Protection Reguliation implementada em maio de 2018 nos países que compõe a Área Econômica Europeia), e o que temos visto na Europa é que a Autoridade Supervisora, também tem uma atuação consultiva, inclusive levanta recursos financeiros através de consultorias a empresas privadas, o que tem se mostrado uma alternativa sustentável, uma vez que dessa forma a Autoridade Supervisora não depende do recebimento de multas para se auto financiar. Mesmo assim multas milionárias já foram aplicadas pela GDPR a grandes empresas da Europa, como por exemplo no caso da gigante da aviação a empresa British Airways que foi multada em US$230 milhões por vazamento de dados pessoais de parte de seus clientes.

O ICO (Information Comissioner's Office) uma instituição independente do Reino Unido tem sido uma das principais fontes de suporte, consulta e compartilhamento de documentações voltadas a suportar as empresas nessa jornada de adesão as medidas de proteção de dados pessoais. Em seu site (www.ico.org.uk) é possível encontrar desde respostas a dúvidas frequentes até modelos prontos para uma Política de Segurança de Informação, Template para avaliação de impacto, entre outras documentações que estão ajudando as empresas na Europa a se adequarem a GDPR e certamente também irão contribuir com as empresas no Brasil para atenderem as medidas exigidas pela LGPD.

O que temos visto no Brasil é o crescente mercado de "Advogado de Porta de Data Center", termo que tem se tornado comum principalmente entre as empresas privadas, que tem sido constantemente bombardeada de tudo que é lado pelos mais diversos tipos de Escritórios de Advocacias, que tem visto na LGPD um novo nicho de mercado.

Além de escritórios especializados também está crescendo o número de treinamentos e certificações voltadas a esse novo perfil de profissional, que deve misturar um amplo conhecimento em governança de segurança da informação, com o conhecimento não só na lei, mas no modo geral em que o Poder Legislativo trabalha no Brasil.

Mas independente do setor de atuação ou do porte da empresa, certamente o primeiro passo que as empresas deverão dar é nomear as pessoas que serão encarregadas de estudar esse assunto, essas pessoas deverão antes de mais nada ler a Lei que está publicada sob o número 13.709 disponível gratuitamente a todos no site da Presidência da República (www.planalto.gov.br). Depois que estiverem familiarizada não só com os termos da LGPD, mas principalmente em como navegar pelos seus artigos, ai sim terão uma base mínima para começar a construção e o desenvolvimento de um Programa de Proteção e Privacidade, o que certamente será amplamente utilizado tanto para auxiliar a empresa na priorização de adoção de medidas de segurança, quanto para apresentação de evidências quando e se forem solicitadas.

2 **ESTRUTURA FUNCIONAL**

A estrutura funcional da LGPD envolve 4 elementos, sendo a Autoridade Nacional de Proteção de Dados (ANPD), o Controlador, o Processador, o Encarregado de Proteção de Dados (DPO) e o Titular dos Dados.

2.1. Autoridade Nacional de Proteção de Dados

Entidade governamental que reporta diretamente para a Presidência da República, tem papel consultivo, liberdade técnica, investigatória e corretiva, ou seja, a ANPD deverá prestar consultoria para as empresas que eventualmente venha expor situações de risco identificadas após uma avaliação de riscos e também validar medidas de segurança voltadas a proteção de dados pessoais envolvidos em determinados processos, servirá como ponto centra para recebe denúncias quanto a possíveis irregularidades, terá o poder de definir e aplicar penalidades, que poderão ser desde uma simples advertência, até multas que podem chegar no valor de R$50 milhões por infração (ou até 2% do faturamento da empresa).

2.2 Controlador

É quem coleta e processa os dados dos Titulares, e tem a responsabilidade de defini a finalidade de processamento, categorizar os dados coletados, os titulares e outros.

Além disso o Controlador também é responsável pelo tratamento e adoção das medidas de segurança voltada a proteção de dados pessoais e a garantia da privacidade, para isso deverá realizar avaliações de impacto de proteção de dados, manter um registro das atividades de processamento, garantir a coleta minimizada de dados pessoais, reparar danos causados devido a violação de dados e Informar a ANPD caso haja violação de dados pessoais.

2.3. Processador

Também chamado de OPERADOR, é quem realiza o tratamento de dados em nome do Controlador e tem a responsabilidade de manter o registro das atividades de processamento, detalhar as categorias de processamento de dados, implementar medidas técnica e organizacionais para proteção de dados, informar o Controlador caso haja uma violação de dados pessoais e reparar danos causados devido a violação de dados.

2.4 Encarregado de Proteção de Dados Pessoais

Mais conhecido como DPO (sigla adotada na Europa para *Data Protection Officer*), é uma nova função criada pela LGPD que deverá necessariamente estar presente em todos os Controladores que coletam e processam dados de pessoa Física, porém essa função não é exigida para os Processadores.

A principal função do DPO é de atua como interlocutor entre o Controlador, os Titulares de dados e a ANPD. Deverá ser envolvido em todas as questões de proteção de dados pessoais, terá que monitorar conformidade legal, aconselhar o Controlador, orientar quanto a realização de avaliação de impacto sobre dados pessoais (AIPD), promover programas de treinamento para pessoal, entre outras atribuições.

Para se nomear um DPO deve se considerar que esse pode ser um Colaborador, desde que não haja conflito de interesse e que esse tenha total liberdade para exercer suas atividades (inclusive de reportar a ANPD situações de risco em que a empresa está envolvida), mas a função do DPO poderá ser realizada por um Terceiro ou contratada como um serviço. Um ponto de suma importância é que o DPO esteja ligado diretamente a Alta Diretoria / Time Executivo.

2.5 Titular

Pessoa física dona de fato das informações tratadas pelo Controlador, através da LGPD passará a ter garantido por lei os seguintes direitos no que se refere a coleta, armazenamento e processamento de seus dados pessoais:

1. Confirmação da existência de tratamento
2. Acesso aos dados
3. Correção de dados incompletos, inexatos ou desatualizados
4. Anonimização, bloqueio ou eliminação de dados
5. Portabilidade dos dados a outro fornecedor
6. Eliminação dos dados (esquecimento)
7. Informações sobre o compartilhamento de dados com terceiros
8. Informações sobre a possibilidade de não fornecer o consentimento
9. Revogação do consentimento

3 **FUNDAMENTOS LEGÍTIMOS**

Um dos principais pilares da LGPD os FUNDAMENTOS LEGÍTIMOS, é formado por uma lista de condições as quais o Controlador deverá atender para tornar legal sua atividade de coleta, processamento e/ou armazenamento de dados pessoais.

Abaixo quais são essas condições:

1. Finalidade: Propósito legítimo, específico, explicito e informado ao Titular
2. Adequação: Processamento restrito apenas a finalidade informada ao Titular
3. Necessidade: Processar o mínimo necessário de acordo com a finalidade
4. Livre acesso: Garantir ao Titular acesso facilitado e gratuito aos seus dados
5. Qualidade dos dados: Os dados devem ser claros, exatos e atualizados
6. Transparência: Informações claras e precisas quanto aos tratamentos aplicados
7. Segurança: Adoção de medidas técnicas e organizacionais para proteção dos dados
8. Prevenção: Ações preventivas quanto a violações de segurança
9. Não discriminação: Proibido uso de dados para fins discriminatório, ilícitos ou abusivo
10. Responsabilização: Demonstração das medidas adotadas para o cumprimento da LGPD

4 **FINALIDADE**

Outro pilar essencial para sustentação da LGPD trata da FINALIDADE do tratamento dos dados pessoais, ou seja, o Controlador deverá estar embasado em no mínimo uma das finalidades definidas pela LGPD para que possa realizar legalmente suas atividades que envolvam coleta, processamento e/ou armazenamento de dados pessoais.

O tratamento de dados pessoais só poderá ser realizado em no mínimo uma das seguintes hipóteses:

1. Consentimento do Titular (*mais difícil de ser implementado);
2. Cumprimento de obrigação legal ou regulatória;
3. Pela Administração Pública para a execução de política pública;
4. Pesquisa científica, garantindo a anonimização dos dados;
5. Execução de contrato;
6. Processo judicial, administrativo ou arbitral;
7. Proteção da vida (quando há risco de morte);
8. Tutela da saúde realizado por serviço de saúde ou autoridade sanitária;
9. Interesse legítimo do Controlador (*maior margem para discussão);
10. Proteção de crédito

Mesmo assim, se a atividade de tratamento de dados envolva dados que revelem a origem racial ou ética, opção religiosa, filosófica, política, sexual, filiação sindical, dados de saúde, biológicos ou genéticos do Titular, classificados na LGPD como Dados Sensíveis, o tratamento só poderá se dar em caso de:

1. Consentimento do Titular para finalidade específica
2. Cumprimento de obrigação legal ou regulatória;
3. Execução de políticas públicas;
4. Pesquisa cientifica (homologada por academias);
5. Declaração de defesa em processo judicial;
6. Proteção da vida do Titular;
7. Tutela da saúde realizado por serviço de saúde ou autoridade sanitária;
8. Prevenção a fraude e a segurança do Titular.

5 **GOVERNANÇA**

Além dos fundamentos legítimos e da finalidade, a LGPD estabelece que o CONTROLADOR e OPERADOR deverão adotar programa de governança em privacidade capazes de demonstrar comprometimento em adotar práticas de proteção de dados e que abranja todos os dados pessoais independente de quem realizou a coleta.

O programa de governança deverá ser compatível a estrutura e volume das operações de cada empresa, ou seja, o plano de governança deverá ser estabelecido e implementado de acordo com o porte da empresa, o setor em que atua, suas condições financeiras, as normas e legislações que estão submetidas entre outros.

O principal é que cada empresa estabeleça políticas e salvaguardas adequadas com base em processo de avaliação de impacto e risco a privacidade, a fim de criar uma relação de confiança com o Titular dos dados, por meio de atuação clara, justa e transparente.

O mais recomendado é que dentro da estrutura de governança geral da empresa, exista um Programa de Proteção de Privacidade (PPP) que além das definições das medidas técnicas e organizacionais voltadas a mitigação de riscos, também contemple um plano de resposta a violações e remediações, além de monitoramento constante que garanta melhoria continua a esse programa.

Por isso, uma das abordagens recomendadas para estabelecer um PPP é a implementação de um Sistema de Gestão de Proteção de Dados (SGPD) baseado na metodologia PDCA (Plan Do Check Act), que estabelece fazes sequenciais capazes de definir, implementar e melhorar as medidas técnicas e organizacionais voltadas a proteção de dados pessoas. São 5 as etapas de um SGPD: 1º) Preparação; 2º) Organização; 3º) Desenvolvimento e Implementação; 4º) Governança; 5º) Avaliação e Melhoria.

5.1. Preparação

Propósito: Preparar a Organização para proteger a privacidade.

Objetivos: Analisar os requisitos e necessidade de proteção de Dados Pessoais; Coletar leis, regulamentos e normas; Estabelecer um plano de ação;

Etapas:

1. Realizar análise de privacidade
2. Coleta de leis de privacidade e análise do impacto da privacidade para a organização
3. Estabelecer organização de Governança de Dados.
4. Realizar auditorias dos Dados Iniciais
5. Realizar o Registro de Atividades de Processamento (Processing Activities Register)
6. Realizar avaliações (checklist) e auditorias dos Dados Iniciais
7. Estabelecer programas de Privacidade e Proteção de Dados.

5.2. Organização

Propósito: Estabelecer estruturas organizacionais e mecanismos para as necessidades de privacidade da organização.

Objetivos: Desenhar e implantar o programa de proteção de dados e privacidade; Designar e anunciar o DPO; Envolver e obter o compromisso de todas as partes interessadas relevantes;

Etapas:

1. Manter programa, políticas e controles de governança de privacidade de dados
2. Atribuir e manter responsabilidades ao Programa de Proteção de Dados Pessoais (PPDP)
3. Gerenciar o envolvimento da gerência sênior no Programa de Proteção de Dados Pessoais (PPDP)
4. Manter o compromisso da organização com PPDP
5. Manter comunicação regular para questões de PPDP
6. Manter o engajamento das partes interessadas no PPDP
7. Implementar e operar sistemas computadorizados de PPDP

5.3. Desenvolvimento e Implementação

Propósito: Desenvolver e implementar medidas e controles específicos para o Programa de Proteção de Dados e Privacidade (PPDP).

Objetivos: Projetar um sistema de classificação de dados; Desenvolver e implementar políticas, procedimentos e controles para cumprir leis de privacidade e requisitos da organização; Etapas:

1. Desenvolver e implementar estratégias, planos e políticas do PPDP

Implementar o procedimento de aprovação para processamento de Propósito: Estabelecer mecanismos de governança de privacidade.

Objetivos: Desenhar e configurar estruturas de governança. – Ex.: Programa de proteção e privacidade, DPO, etc.; Envolver e obter o comprometimento de todas as partes interessadas relevantes; Relatar todas as questões de privacidade (processo contínuo).

Etapas:

1. Implementar práticas para gerenciar o uso de dados pessoais
2. Manter avisos de privacidade sobre dados pessoais
3. Executar um plano de solicitações, reclamações e retificações
4. Executar uma avaliação de riscos de proteção de dados
5. Emitir relatórios do PPDP
6. Manter documentação de privacidade de dados
7. Estabelecer e manter um plano de resposta de violação de privacidade
2. dados pessoais
3. Registrar bancos de dados para dados pessoais
4. Desenvolver e implementar um sistema de transferência internacional de dados
5. Executar atividades de integração do PPDP

Executar o plano de treinamento do PPDP

5.4. Governança

Propósito: Estabelecer mecanismos de governança de privacidade.

Objetivos: Desenhar e configurar estruturas de governança. – Ex.: Programa de proteção e privacidade, DPO, etc.; envolver e obter o comprometimento de todas as partes interessadas relevantes; Relatar todas as questões de privacidade (processo contínuo).

Etapas:

8. Implementar práticas para gerenciar o uso de dados pessoais
9. Manter avisos de privacidade sobre dados pessoais
10. Executar um plano de solicitações, reclamações e retificações
11. Executar uma avaliação de riscos de proteção de dados
12. Emitir relatórios do PPDP
13. Manter documentação de privacidade de dados
14. Estabelecer e manter um plano de resposta de violação de privacidade

5.5. Avaliação e Melhoria

Propósito: Avaliar e melhorar todos os aspectos específicos de proteção de dados e privacidade da organização (controles, políticas, procedimentos, práticas, etc.).

Objetivos: Monitorar a operação e a resolução de todas as questões relacionadas à privacidade; Avaliar regularmente a conformidade com processos e políticas internas;

Melhorar a proteção de dados e as medidas de privacidade;

Etapas:

1. Realizar auditoria interna de PD & P
2. Envolver uma parte externa para avaliações PD & P
3. Realizar avaliações e estabelecer benchmarks (comparações)
4. Executar avaliações de riscos de proteção de dados
5. Resolver riscos do PPDP
6. Relatar análise de riscos do PPDP e resultados
7. Monitorar as leis e regulamentos do PPDP

5 **CONSIDERAÇÕES FINAIS**

Esse estudo busca estabelecer um modelo de trabalho que possa servir como referência para os profissionais responsáveis pela definição e implementação de medidas técnicas e organizacionais, voltadas a atender as exigências estabelecidas na LGPD, a fim de respeitar o direito a vida privada de cada cidadão em seu âmbito familiar, garantido assim seu amplo direito a liberdade.

REFERÊNCIAS

Foundations of Information Security – Based on ISSO 27001 and ISO 27002. Van Haren, Publishing 2015. ISBN 978 94 018 0012 9.

Congresso Brasileiro Lei Geral de Proteção de Dados (LGPD) (Lei n. 13.709/2018) Brasília, 14 de agosto de 2018.

European Commission. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Patricia Peck Pinheiro Proteção de Dados Pessoais - Comentários à Lei n. 13.709/2018 (LGPD) Saraiva Jur, edição: 1ª (23 de novembro de 2018) ISBN-13: 9788553605286.

Márcio Cots, Ricardo Oliveira Lei Geral de Proteção de Dados Comentada Revista dos Tribunais, edição: 1ª (23 de outubro de 2018) ISBN-10: 8553212122 ISBN-13: 9788553212125.

Bruno Ricardo Bioni Proteção de Dados Pessoais: a função e os limites do consentimento Editora Forense, edição: 1ª (29 de outubro de 2018).

A. Calder EU GDPR A pocket guide IT Governance Publishing ISBN 978-1-84928-855-2; L. Besemer White Paper – Privacidade, Dados Pessoais e GDPR.

European Commission General Data Protection Regulation (GDPR) Regulation of the European Parliament and the Council of the European Union. Brussels, 6 April 2016.

IT Governance Privacy Team. EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide.

Kyriazoglou, J. Data Protection and Privacy Management System. Data Protection and Privacy Guide Vol. 1 bookboon.com primeira edição (2016).