LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: Desafios e impactos para o Poder Público*

GENERAL LAW ON PERSONAL DATA PROTECTION: Challenges and impacts for the Public Power

Charles Rogério Vasconcelos[1]
Marta Luiza Leszczynski Salib[2]

RESUMO

O advento da Lei Geral de Proteção de Dados Pessoais (LGPD) trouxe imposição normativa para que instituições públicas e privadas, que realizem tratamento de dados pessoais, se adequem à referida Lei. O presente artigo, tem como foco demonstrar os desafios e impactos a serem enfrentados pelo Poder Público na busca por conformidade à LGPD. A metodologia de pesquisa utilizada é qualitativa, descritiva e bibliográfica, utilizando-se do método dedutivo na fase de investigação. Assim, pôde-se perceber a complexidade e imprescindibilidade de se construir uma cultura organizacional e diretrizes de boas práticas e governança, que devem nortear ações referentes ao tratamento de dados pessoais no âmbito da organização.

Palavras-Chave: Lei Geral de Proteção de Dados. Poder Público. Desafios. Políticas de Segurança. Sanções.

ABSTRACT

The advent of the General Law on the Protection of Personal Data (LGPD) brought normative imposition for public and private institutions, that carry out the treatment of personal data, to comply with the referred Law. This article focuses on demonstrating the challenges and impacts to be faced by the Public Power in the search for LGPD compliance. The research methodology used is qualitative, descriptive and bibliographic, using the deductive method in the investigation phase. Thus, it was possible to perceive the complexity and indispensability of building an organizational culture and guidelines of good practices and governance, which should guide actions related to the treatment of personal data within the organization.

Key Words: General Data Protection Law. Public Power. Challenges. Security Policies. Sanctions.

---

* Artigo desenvolvido como Trabalho de Conclusão de Curso como requisito parcial para obtenção do grau de bacharel em Direito da Faculdade Católica de Rondônia.

[1] Acadêmico do Curso de Direito da Faculdade Católica de Rondônia: E-mail: charles.vasconcelos@sou.fcr.edu.br

[2] Advogada. Doutoranda em Direito e Docente da disciplina de Direito Constitucional da Faculdade Católica de Rondônia. Orientadora do trabalho. E-mail: marta.salib@fcr.edu.br.

INTRODUÇÃO

A Lei 13.709[3] de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, entrou em vigor no dia 18 de setembro de 2020, com aplicação de sanções administrativas apenas a partir de 01 de agosto de 2021.

Portanto, a partir de sua vigência, qualquer pessoa natural ou jurídica de direito público ou privado que realize tratamento de dados pessoais deverá estar em conformidade com os preceitos trazidos pelo normativo legal. E isso acarreta dizer que, os dados das pessoas naturais que estiverem sob custódia desses agentes de tratamento, deverão estar protegidos através da "utilização de medidas 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 difusão." [4]

Desta forma, é mister afirmar, que toda pessoa natural ou pessoa jurídica de direito público ou privado, que incorra na realização de tratamento de dados pessoais deve estar em conformidade com a LGPD.

Para tanto, os desafios são inúmeros e serão abordados no decorrer deste artigo, mas antes de adentrarmos nas minúcias dessa seara, se faz necessário o entendimento de todo contexto que envolve um cenário de busca por *compliance*[5] à Lei Geral de Proteção de Dados Pessoais. Segundo TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. 2019, p. 683),

> Para compreender a relevância que os programas de *compliance* assumem na tutela da proteção dos dados pessoais e no direcionamento dos agentes de tratamento a respeito das condutas necessárias para atender aos preceitos legais, bem como determinar as linhas gerais que devem ser observadas no que se refere à LGPD, afigura-se fundamental determinar o que se entende por *compliance*, suas funções e o conteúdo de tais programas.

Assim, é perceptível a necessidade de as organizações entenderem o que é "estar em *compliance*" com a LGPD, para então, conhecer a conjuntura que estarão inseridas a partir do momento que realizarem tratamento de dados pessoais, e principalmente, quais desafios

---

[3] LGPD art. 1º: Lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado, tendo em vista a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[4] Art. 6º, VII da Lei n. 13.709/2018.

[5] Compliance: "Trata-se da estruturação de políticas e procedimentos corporativos que se traduzem em ações sistemáticas com o objetivo de atender ao cumprimento aos preceitos normativos, a permitir a prevenção do ato ilícito ou, caso tal não seja possível, minorar seus efeitos e sancionar eventuais responsáveis" (TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. Sã Paulo: Thomson Reuters Brasil, 2019. p. 683).

enfrentarão e os possíveis impactos no negócio, seja através do recebimento de sanções administrativas, pela perda de credibilidade perante a sociedade, ou ainda, com a judicialização de demandas nas esferas cível e penal. É nesse cenário que se faz necessário identificar os desafios decorrentes de um processo para aplicação de boas práticas e de governança em privacidade, conforme preconizado no art. 50[6] do referido ordenamento.

Ademais, estar em *compliance* com os requisitos da LGPD exigirá, entre outros aspectos, adequação dos processos organizacionais existentes, demandando, via de regra, investimentos em consultoria especializada, em capacitação de pessoal, em ferramentas de segurança, no mapeamento de dados[7] (*data mapping*), na melhoria de procedimentos e nos fluxos internos e externos acerca de dados pessoais, bem como, na implementação de uma cultura organizacional voltada para a segurança da informação e privacidade.

Portanto, na busca por conformidade, as organizações deverão definir estratégias de proteção de dados com apoio de pessoas e tecnologias que permitam aos seus gestores e colaboradores, alcançarem o nível adequado de governança em privacidade e segurança da informação exigido pela Lei.

Nesse diapasão, não há como discorrer acerca dos desafios e impactos da LGPD no poder público, sem dedicarmos preliminarmente um momento de destaque para questões relativas à segurança da informação e privacidade, abarcando conceitos fundamentais e princípios basilares do tema em epígrafe.

Sendo assim, o objetivo deste estudo é analisar a importância desse "novo" contexto legal em que está inserida a pessoa jurídica de direito público quando realiza operação de tratamento de dados pessoais, e consequentemente, as questões relativas à proteção de dados e privacidade previstas na LGPD, harmonizadas com a Lei nº 12.527/2011[8], em consonância com as normas técnicas da família ISO 27000[9], todas intrinsicamente conectadas através de uma relação umbilical em se tratando do poder público.

Seguindo essa premissa, a primeira parte do artigo abordará questões relacionadas ao valor da informação, termos e conceitos utilizados, e ainda, seu ciclo de vida. Em um segundo

---

[6] Art. 50 da Lei n. 13.709/2018.

[7] Mapeamento de Dados: documento essencial quando da execução do processo de adequação às normas de proteção de dados. O mapeamento deve refletir o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais o dado transita.

[8] Lei de Acesso à Informação: Dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

[9] Família de Normas ISO 27000: Conjunto de normas, em que cada uma possui uma função específica, mas todas têm como principal objetivo a criação, manutenção, melhoria, revisão, funcionamento e análise de um Sistema de Gestão de Segurança da Informação.

momento, trataremos sobre segurança da informação nas organizações, seus princípios fundamentais, os conceitos de incidentes de segurança, as ameaças, vulnerabilidades e riscos que rondam as organizações, o contexto das políticas de segurança da informação nesse cenário, bem como, a necessidade de criação de uma cultura organizacional sobre o tema.

Por fim, será feita abordagem dos principais desafios a serem enfrentados pelo poder público na busca por conformidade à LGPD, seus aspectos gerais, a necessidade de harmonização com outros institutos, e ainda, as responsabilidades, os impactos e possíveis sanções a que estão sujeitos os agentes de tratamento de dados pessoais em caso de descumprimento do ordenamento jurídico.

1 - O VALOR DA INFORMAÇÃO

A informação, cada vez mais, vem se mostrando o ativo de maior valor para uma organização, e por ser valioso, este ativo está sujeito às inúmeras ameaças existentes no ambiente, interno e externo, que podem explorar vulnerabilidades, e assim, comprometer o negócio da organização.

É inequívoco que, com o acelerado desenvolvimento tecnológico que se observa na atualidade, há cada vez mais dispositivos que se propagam pelo espaço urbano, capazes de coletar dados sobre as pessoas, monitorar e vigiar suas atividades e até mesmo manipular seus comportamentos[10].

O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos[11]

Portanto, a organização, pública ou privada, depende da informação para seus processos decisórios, não pode funcionar sem uma quantidade significativa de informação e o seu conhecimento acontece pela utilização do recurso informado. Sem a informação não existe conhecimento, compartilhamento de conhecimento e crescimento corporativo.[12]

Desta forma, esse ativo tão valioso necessita ser protegido. No entanto, se essa

[10] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 499.
[11] Norma Brasileira ISO/IEC 27002:2013: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.
[12] FONTES. Edison. Políticas e Normas para a Segurança da Informação. p. 1 (apud Silva e Tomaél (2007).

informação se refere a dado pessoal[13], os cuidados a serem tomados para proteção e salvaguarda desse ativo, são obrigatoriamente, ainda maiores, pois com o advento da Lei Geral de Proteção de Dados Pessoais, temos a figura do titular do dado[14], que é possuidor de direitos e garantias fundamentais. No Brasil, a tutela jurídica da privacidade, inclusive dos dados pessoais, possui previsão na Constituição Federal[15].

Portanto, a proteção e salvaguarda dessas informações que são tratadas já não é de interesse apenas da organização, e a promoção de ações pertinentes à privacidade e proteção de dados pessoais que estejam sob sua tutela não é mais facultativo, seja a organização pessoa jurídica de direito público ou privado, pois a partir da vigência da LGPD, trata-se de uma imposição legal[16].

1.1 - Termos e o Conceito de Informação

Para entender o que realmente se encaixa no conceito de informação, é preciso diferenciar de outros termos comumente utilizados.

A definição do termo "ativo" é importantíssima neste cenário, e podemos conceituá-lo como sendo qualquer coisa que tenha valor para a organização e para os seus negócios. Alguns exemplos de ativos são: banco de dados, *softwares*, equipamentos (computadores e *notebooks*), servidores, elementos de redes (roteadores, *switches*, entre outros), pessoas, processos e serviços.[17]

É possível conceituar o termo "dado" como sendo uma informação existente antes do seu tratamento,[18] e o termo "informação", é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegido.[19]

---

[13] Art. 5º da Lei n. 13.709/2018. Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; (...).

[14] Art. 5º da Lei n. 13.709/2018. Para os fins desta Lei, considera-se: V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

[15] Art. 5º da Constituição Federal. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[16] Art. 6º da Lei n. 13.709/2018. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VII - segurança: utilização de medidas 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 difusão.

[17] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002**.** p. 2.

[18] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 386.

[19] Norma Brasileira ISO/IEC 27002:2013: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

Assim, é possível dizer que, informação é ativo cada vez mais valorizado [...], representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa.[20]

A informação pode existir em diversos formatos: impressa, armazenada eletronicamente, falada, transmitida pelo correio convencional de voz ou eletrônico etc. Seja qual for o formato ou meio de armazenamento ou transmissão, recomenda que ela seja protegida adequadamente. Sendo de responsabilidade da segurança da informação protegê-la de vários tipos de ameaças, visando garantir a continuidade do negócio, minimizar riscos e maximizar o retorno dos investimentos.[21]

A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação [...], porém a segurança da informação permanece importante [...].[22]

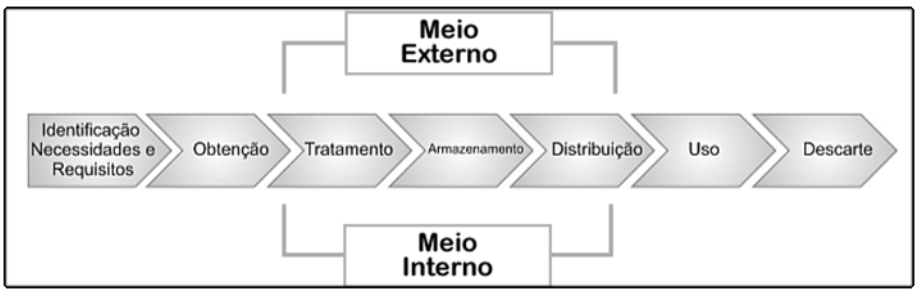

Figura 2: Ciclo de Vida da Informação. (Fonte: Lyra, 2008)

É possível observar na figura 2, que a identificação das necessidades e requisitos é condição fundamental para o ciclo de vida da informação, pois é a partir daí que se deve construir o fluxo da informação no ambiente organizacional. A referida figura também nos mostra as etapas em que se deve aplicar segurança à informação, e ainda, a existência de relacionamento entre a Obtenção e Distribuição da informação com o Meio Externo e Interno à organização.

Desta forma, se faz necessário, entendermos questões conceituais acerca de segurança da informação, bem como, seus princípios, as ameaças, vulnerabilidades e riscos que rondam o dia a dia das organizações.

---

[20] SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. p. 37.
[21] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002**.** p. 2.
[22] Norma Brasileira ISO/IEC 27002:2013: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

2 - SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

A segurança da informação é um ponto crítico para a sobrevivência de qualquer organização que integre a sociedade da informação. Como veremos, os ativos de uma organização estão sujeitos a ameaças internas e externas, que podem explorar desde vulnerabilidades tecnológicas de *softwares*[23] e *hardwares*[24], até humanas, a partir de funcionários despreparados para atuar nesse contexto organizacional. As organizações precisam implantar um processo de segurança da informação, e este processo deve ser considerado um ativo da organização, como tantos outros.[25]

No quesito das práticas de segurança da informação, as empresas devem se basear nas diretivas das melhores instituições de reputação global, como a ISO[26] e o NIST[27], que são entidades de referência mundial com constantes publicações técnicas, funcionando como verdadeiros guias para as melhores práticas consolidadas no âmbito do entendimento global de maturidade em segurança da informação. Muitas associações buscam contribuir com a formulação de guias para o mercado, a exemplo da TeleTrust, associação alemã composta de membros da indústria, administração, consultoria e pesquisa, bem como organizações parceiras com objetivos semelhantes, que formularam um guia do estado da arte[28] em segurança da informação com base nas normas ISO/IEC das famílias 270xx, visando atender ao General Data Protection Regulation - GDPR[29], legislação de proteção de dados da União Europeia.[30]

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os

---

[23] É um programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual.
[24] É um termo técnico que foi traduzido para a língua portuguesa como equipamento. O termo "hardware" é bastante utilizado, principalmente na área de engenharia de computação.
[25] FONTES, Edison. Políticas e Normas para a Segurança da Informação. p. 4.
[26] ISO. Organização não-governamental internacional, que reúne mais de uma centena de organismos nacionais de normalização. Disponível em: [www.portaleducacao.com.br/conteudo/artigos/educacao/a-historiadaorganizacao-iso/40732]. Acesso em 30.10.2020.
[27] NIST. *National Institute os Standards and Technology U.S. Department of Commerce*. Disponível em: [www.nist.gov/]. Acesso em 30.10.2020.
[28] TeleTrust. *State of the art.* Disponível em: [www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/]. Acesso em 30.10.2020.
[29] GDPR. Regulamento Geral sobre a Proteção de Dados da União Europeia. Disponível em português em: [https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT]. Acesso em 30.10.2020.
[30] MALDONADO, Viviane Nóbrega. LGPD Lei Geral de Proteção de Dados Pessoais – Manual de Implementação. p. 342.

objetivos do negócio e a segurança da informação da organização são atendidos.[31]

Mudanças nos processos e sistemas do negócio ou outras mudanças externas (tais como novas leis e regulamentações), podem criar novos riscos de segurança da informação. Desta forma, em função das várias maneiras nas quais as ameaças podem se aproveitarem das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz estes riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos.[32]

Importante ressaltar, que são inúmeros os conceitos e definições acerca de segurança da informação, tendo como ponto de partida a conceituação[33] expressa na norma brasileira NBR ISO/IEC 27002 que trata especificamente do assunto. No entanto, aqui abordaremos apenas o essencial para que se tenha uma noção básica e introdutória sobre o tema, intrinsicamente conectado aos preceitos da Lei Geral de Proteção de Dados de Pessoais.

Observe-se que a definição do conceito de "segurança da informação" é mais, ou menos complexa, de acordo com a visão de alguns autores.

Patrícia Peck, afirma que o maior desafio do governo brasileiro é assegurar a atualização tecnológica da própria Administração Pública, num contexto de mudança e inovação aceleradas, sobretudo por meio da identificação e da gestão das competências essenciais ao governo eletrônico,[34] e ainda, que informação é um ativo intangível, e sendo assim, deduz-se que esteja sujeita a diversas ameaças, tais como: acesso indevido; furto de informações; fraude eletrônica e falsificação de identidade; dano aos dados e informações arquivadas; espionagem para obtenção de segredos industriais/comerciais; cópia de programa; violação de direito autoral; interceptação indevida de informação; e violação de base de dados pessoais.[35]

É possível definir segurança da informação como sendo uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade, ou ainda, como sendo a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais princípios da segurança:

---

[31] Norma Brasileira ISO/IEC 27002:2013: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.
[32] Norma Brasileira ISO/IEC 27002:2013: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.
[33] ISO/IEC 27002:2013: A proteção da informação contra os mais diversos tipos de ameaças para garantir a continuidade dos negócios, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio, preservando a confidencialidade, a integridade e a disponibilidade da informação.
[34] PINHEIRO. Patrícia Peck. Direito Digital. p. 152
[35] PINHEIRO. Patrícia Peck. Direito Digital. p. 101

confidencialidade, integridade e disponibilidade da informação.[36]

Portanto, a aplicação de segurança da informação é determinante para assegurar competitividade, lucratividade, atendimento aos requisitos legais e a imagem da organização junto ao mercado, às organizações, tanto no setor público quanto no setor privado.[37]

2.1 - Princípios Fundamentais da Segurança da Informação

A segurança da informação tem como objetivo maior a preservação de três princípios básicos que norteiam a implementação dessa prática, visando garantir a tríade Confidencialidade, Integridade e Disponibilidade (CID), que pode ser conceituada da seguinte forma:

Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas ás pessoas a quem é destinada; **Integridade**: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protege-la contra alterações indevidas, intencionais ou acidentais; **Disponibilidade**: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que eles necessitam dela para qualquer finalidade.[38]

Em suma, pode-se definir a tríade CID de forma simplificada da seguinte maneira: Confidencialidade: a informação só deve ser acessível a quem tem a devida autorização; Integridade: a informação deve manter-se inalterada desde sua geração ou alteração autorizada; e, Disponibilidade: a informação deve estar sempre disponível às pessoas autorizadas.

No que se refere a qual seria o nível de segurança requerido para executar os princípios da segurança da informação na organização, é possível afirmar que, é diferente para cada organização, pois cada uma tem sua própria combinação de objetivos e requisitos de negócio e de segurança. Todos os controles de segurança, mecanismos e proteções são implementados para prover um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são medidos pela sua capacidade potencial de comprometer um ou todos os princípios do triângulo CID.[39]

Portanto, é necessário que as organizações públicas e privadas, busquem proteção

---

[36] SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. p. 41.
[37] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002.
[38] SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. p. 43.
[39] BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.

contra possíveis eventos de segurança da informação, que é a ocorrência identificada de um estado de um sistema, serviço ou rede que indique uma possível violação da política de segurança da informação ou falha de proteção, ou uma situação previamente desconhecida que possa ser relevante em termos de segurança.[40]

2.2 - Incidente de Segurança

Um incidente de segurança pode ser definido como fato (evento) decorrente da ação de uma ameaça, que explora uma vulnerabilidade, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.[41]

O desenvolvimento de qualquer processo em segurança da informação começa, invariavelmente, com a definição de um problema a ser resolvido. Quando levamos essa definição para o universo da resposta a incidentes, é natural procurar responder qual problema esperamos que a resposta a incidentes resolva. Minimizar os danos penso ser uma boa resposta tendo em vista que, se um incidente de segurança acontecer, algum dano ele vai causar.[42]

A Lei Geral de Proteção de Dados Pessoais, traz que "o controlador[43] deverá comunicar à autoridade nacional[44] e ao titular[45] a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares". O mesmo instituto impõe, ainda, a obrigação legal para que o controlador "conte com planos de resposta a incidentes e remediação".[46]

Assim, na hipótese de vazamento de dados, invasão do sistema ou incidentes similares, que possam acarretar risco ou dano relevante aos titulares, o respectivo controlador deve informar aos envolvidos, bem como ao órgão responsável, sobre o ocorrido, de modo a dar ciência da extensão do dano e possibilitar a mitigação das consequências dele advindas.[47]

Para tanto, se faz necessário identificar alguns conceitos de fatores preponderantes que

---

[40] BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.
[41] SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. p. 48.
[42] MALDONADO. Viviane Nóbrega. LGPD Lei Geral de Proteção de Dados Pessoais – Manual de Implementação. p. 340.
[43] Art. 48, VI da Lei n. 13.709/2018. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
[44] Art. 48, XIX da Lei 13.709/2018. Autoridade Nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
[45] Art. 48, V da Lei 13.709/2018. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
[46] Art. 50, § 2º, inciso I, alínea "g" da Lei 13.709/2018.
[47] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 177.

contribuem para a ocorrência de incidentes de segurança, visto que, nos dias de hoje, vivemos em um mundo rodeado de tecnologias, altamente conectado e repleto de ameaças digitais. Sequestro de informações, passando por engenharia social, códigos maliciosos, funcionários despreparados, espionagem, crime cibernético cada vez mais sofisticado, essas e outras ameaças podem causar sérios danos a uma organização. Promover ações de proteção de dados pessoais e informações críticas e reduzir riscos devem ser práticas constantes nas organizações.[48]

Desta forma, é possível conceituar **ameaça** como sendo qualquer evento que explore vulnerabilidades. Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.[49] É, uma potencial causa de um incidente não desejado, o que pode resultar em prejuízo ao sistema ou à organização.[50]

Vulnerabilidade, é qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações,[51] ou ainda, a fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.[52]

Risco é a combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a organização,[53] ou ainda, a probabilidade de um agente ameaçador tirar proveito de uma vulnerabilidade e o seu respectivo impacto comercial.[54]

Ataque é qualquer ação que comprometa a segurança de uma organização,[55] ou, uma tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a, ou fazer uso não autorizado de um ativo.[56]

O Poder Público precisa estar mais atento às questões de segurança da informação nacional. Os ataques são possíveis porque encontram vulnerabilidades e também pela falta ou precariedade na estratégia de um plano de contingência e continuidade.[57]

A LGPD, entre outros, confere aos agentes de tratamento (isto é, tanto controladores

---

[48] MALDONADO, Viviane Nóbrega. LGPD: Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. p. 208.
[49] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002. p. 3.
[50] BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.
[51] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002. p. 3.
[52] BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.
[53] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002. p. 3.
[54] BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.
[55] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002. p. 3.
[56] BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.
[57] PINHEIRO. Patrícia Peck. Direito Digital.

quanto operadores) o dever de adotar providências concretas de segurança, em nível técnico e administrativo, que se mostrem aptas a resguardar os dados pessoais sobre os quais detêm responsabilidade de vazamentos e/ou tratamento indevido,[58] ou seja, quem se propõe a tratar dados deve possuir, efetivamente, a capacidade de protege-los, evitando ataques e acessos desautorizados, como forma de garantia de segurança das informações coletadas.[59]

2.3 - Políticas de Segurança da Informação

Fundamental característica da nova legislação consiste no significativo fomento ao aspecto preventivo, estabelecendo procedimentos mandatórios para os controladores e operadores de dados pessoais, tais como os deveres atinentes à implementação de severas políticas de segurança para proteção dos dados de acessos não autorizados.[60]

Em muitas instituições, há uma grande preocupação na utilização de mecanismos de proteção eficientes, na elaboração de uma Política de Segurança da Informação - PSI, bem alinhada, com profissionais qualificados, mas frequentemente acabam se esquecendo do elo mais fraco, o ser humano. Que se não estiver preparado e capacitado para enfrentar as ameaças do ambiente interno e externo, pode comprometer todo o processo, revelando informações sensíveis.[61]

Diante deste cenário, importante conceituarmos política de segurança da informação, que é um documento jurídico no modelo de diretriz que traz todas as regras, padrões e procedimentos obrigatórios para proteção dos ativos e atividades da empresa.[62] Objetiva, a definição de direitos e responsabilidades, ou seja, procura-se deixar claro o que cada pessoa ou sistema pode fazer ou não dentro do contexto da organização.[63]

Após instituídas as políticas, normas e procedimentos no ambiente organizacional, é necessário dar publicidade, devendo ser divulgados e constantemente lembrados, possibilitando que os usuários de todas as áreas da organização não tenham dúvidas de como tratar a informação.[64]

Assim, a divulgação e conscientização acerca das políticas, serve tanto para prevenção de incidentes como para proteção da organização no sentido de que capacitou seus

---

[58] Art. 46 da Lei n. 13.709/2018.
[59] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p.175.
[60] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 681.
[61] DELLA VECCHIA, Evandro. Perícia Digital: Da Investigação à Análise Forense. p. 22.
[62] PINHEIRO, Patricia Peck. Direito Digital. p. 120.
[63] DELLA VECCHIA, Evandro. Perícia Digital: Da Investigação à Análise Forense. p. 22.
[64] FONTES, Edison. Políticas e Normas para a Segurança da Informação. p. 135.

profissionais no correto uso da tecnologia. Logo, estes serão responsabilizados caso a utilizem de forma incorreta.[65]

Importante que as políticas instituídas estejam alinhadas com a NBR ISO/IEC 27002, com a legislação vigente e com as normas gerais pelas quais a organização se orienta.[66]

No sentido de construir políticas, o Governo Federal editou o Decreto 9.637/2018, o qual instituiu a Política Nacional de Segurança da Informação (PNSI) no âmbito da Administração Pública Federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional.[67]

Percebe-se que, instituir políticas, normas, procedimentos, e ainda, dar transparência acerca das diretrizes adotadas pela organização no que diz respeito à segurança da informação, não é tarefa fácil, principalmente porque as diretrizes a serem construídas devem abarcar a organização como um todo.

2.4 - Criação de Cultura Organizacional

É fato que nenhuma organização nasce com uma cultura pronta. Ela se constrói ao longo do tempo, direcionada, via de regra, pelo planejamento estratégico da organização em busca de consolidar ações e boas práticas coerentes e materializadas no dia-a-dia de seus colaboradores através de diretrizes, normas e políticas explicitadas e incorporadas aos hábitos individuais de cada pessoa no contexto da organização.

As diretrizes, que por si só, têm papel estratégico, precisam expressar a importância que a empresa dá para a informação, além de comunicar aos funcionários seus valores e seu comprometimento em incrementar a segurança à sua cultura organizacional [...]. A política deve expressar as preocupações dos gestores e definir as linhas de ação que orientarão as atividades táticas e operacionais.[68]

Faz parte das boas práticas conscientizar o usuário quanto a seus direitos e deveres perante os recursos de processamento disponíveis na organização e na legislação vigente. Por exemplo, requerendo dos usuários a assinatura de uma declaração do conhecimento de suas responsabilidades no contexto da organização. E, por conseguinte, manter em segurança tais declarações assinadas.[69]

Neste cenário, complexo, o usuário precisa estar comprometido com a proteção da

---

[65] PINHEIRO, Patricia Peck. Direito Digital. p. 121.
[66] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002.
[67] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 180.
[68] SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma Visão Executiva. p. 105.
[69] COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002.

informação na organização para qual ele trabalha para que o processo de segurança exista de forma eficaz. No processo de treinamento deve-se difundir a política de segurança de informação e ensinar boas práticas para que ele saiba como agir nas diversas situações do dia-a-dia, mesmo naquelas não previstas explicitamente nos procedimentos.[70]

Atender aos requisitos da LGPD, não é tarefa simples, e exige adequação dos processos de governança corporativa, com implementação de um programa consistente de compliance digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura. A LGPD traz um grande impacto social e econômico.[71]

Na Política Nacional de Segurança da Informação, também foi elencada a missão de orientar ações em prol da segurança dos dados custodiados por entidades públicas, bem como, a de fortalecer a cultura da Segurança da Informação no meio social.[72]

Assim, está cristalino a importância da aplicação de ações acerca de segurança da informação para proteção e privacidade de dados nas organizações públicas e privadas, objetivando a criação e o fortalecimento de uma cultura organizacional transversal que envolva os colaboradores internos e externos, através da aplicação de diretrizes e boas práticas de governança em privacidade de dados.

3 - A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD E SUA APLICAÇÃO NO ÂMBITO DO PODER PÚBLICO

3.1 - Aspectos Gerais da LGPD

Organismos internacionais como a OCDE[73] e CoE[74], bloco regionais como União Europeia/EU e diversos países estão modernizando ou editando, pela primeira vez, suas leis de proteção de dados pessoais. Tais variações normativas abrem necessariamente uma nova rodada de discussão sobre nível de convergência dessas normas recentemente promulgadas.[75]

Esse é exatamente o caso brasileiro e europeu. Ambos passaram recentemente por um

---

[70] FONTES, Edison. Políticas e Normas para a Segurança da Informação. p. 186.
[71] PINHEIRO. Patrícia Peck. Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD.
[72] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 180.
[73] OCDE. Organização de Cooperação e de Desenvolvimento Económicos. Disponível em: [https://ec.europa.eu/info/food-farming-fisheries/farming/international-cooperation/international-organisations/oecd_pt]. Acesso em: 31/10/2020.
[74] CoE. Conselho da Europa. Disponível em: [https://www.coe.int/pt/web/about-us]. Acesso em: 31/10/2020.
[75] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 798.

(re)ajuste de suas infraestruturas regulatórias, o que aconteceu no curto espaço de tempo dos últimos 02 (dois) anos. Em 2016, a EU aprovou o Regulamento de Proteção de Dados/RGPD em substituição a antiga diretiva de meados da década de 90. Por sua vez, o Brasil editou, em agosto de 2018, a sua primeira Lei Geral de Proteção de Dados Pessoais,[76]que entrou em vigor em 18 de setembro de 2020.

A data para aplicação das sanções administrativas previstas na LGPD passa a valer a partir de 1º de agosto de 2021, em virtude da aprovação da Lei n. 14.010/20, que prorrogou o prazo inicialmente previsto, por conta da pandemia do coronavírus (Covid-19).

A nova lei, destinada à tutela de direitos fundamentais de liberdade e privacidade de todos os cidadãos, adotou um cunho didático ao trazer definições e conceitos a princípio compreensíveis por toda sociedade.[77] Ela possui 10 capítulos e 65 artigos e estão distribuídos da seguinte forma: Capítulo I apresenta as disposições gerais e traz no art. 2º os princípios que fundamentam a proteção de dados pessoais, no art. 3º a territorialidade de aplicação da lei, no art. 4º é trazido a inaplicabilidade da lei, e no art. 5º temos os conceitos gerais.

A LGPD, pode ser vista como freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas sem a ciência ou o consentimento informado dos usuários.[78] A lei, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[79]

A conformidade à Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais, é hoje o grande objetivo das organizações, e ela deve estar elencada no plano estratégico das corporações. Para atender a essa estratégia, devem ser criados mecanismos no nível do plano tático de forma a dar as diretrizes para as atividades requeridas no nível operacional, justamente onde ocorrem os incidentes de segurança, que necessitam de respostas rápidas e adequadas.[80]

Sendo assim, toda organização deve buscar conformidade legal, e neste caso, se manter

---

[76] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 798.
[77] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 501.
[78] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 103.
[79] Art 1º da Lei n. 13.709/2018.
[80] MALDONADO. Viviane Nóbrega. LGPD Lei Geral de Proteção de Dados Pessoais – Manual de Implementação. p. 341.

atualizada quanto às legislações, normas e padrões de segurança aplicáveis à privacidade e proteção de dados. Em caso de desconformidade, há possibilidade de responsabilização para muito além das infrações relacionadas exclusivamente à Lei Geral de Proteção de Dados Pessoais. Portanto, organizações públicas e privadas, servidores públicos e funcionários devem conhecer suas responsabilidades e atribuições legais inerentes a esse ambiente de alta criticidade ao qual estão inseridos.

3.2 - A LGPD e o Poder Público

O Poder Público existe para administrar a vida em sociedade e o faz somente em observância e na medida em que a lei lhe dá investidura. Significa dizer que o poder público existe para cumprir uma função legal e, para tanto, a lei o investe de poder para fazê-lo.[81]

A Administração Pública ou o Poder Público deverá obedecer a princípios constitucionais que vinculam a sua atuação, preconizados no art. 37 da Constituição Federal [82].

A LGPD, em seu artigo 23, elenca como pessoas jurídicas de direito público as referidas no parágrafo único do art. 1º, incisos I e II da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) demonstrando relação de interação e complementariedade entre as leis. Ocorre que, tais pessoas jurídicas são regidas por legislação específica e submetidas a regulamentos próprios que não abrangem os particulares, motivo pelo qual há tratamento apartado na nova lei para a atuação de tais pessoas jurídicas com dados pessoais.[83]

É correto afirmar que o objetivo da LGPD é o de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". O verbo "proteger" diz muito sobre a forma como o legislador enxergou o titular dos dados, ou seja, em posição desigual em relação aos responsáveis pelo tratamento desses dados, ficando patente sua vulnerabilidade.[84]

3.2.1 - Tratamento de Dados pelo Poder Público

Da mesma forma que as instituições privadas devem apresentar uma finalidade clara e transparente para a realização do tratamento de dados pessoais, a pessoa jurídica de direito público deve adotar a finalidade pública e o interesse público para a realização de tratamento

---

[81] MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. p. 253.
[82] COTS. Márcio, OLIVEIRA. Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. p. 141.
[83] COTS. Márcio, OLIVEIRA. Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. p. 143.
[84] COTS. Márcio, OLIVEIRA. Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. p. 48.

de dados.[85]

Insta salientar que, conforme o art. 7º da LGPD, a Administração Pública pode tratar dados mediante base legal específica (inciso III), não dependendo de consentimento ou enquadramento em outras hipóteses, exceto se mais específica, como é o caso da tutela à saúde.[86]

O art. 49 da referida lei prevê que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e em outras normas regulamentares atinentes ao tema, a exemplo das normativas técnicas.[87]

O tratamento de dados refere-se a toda operação que for realizada com dados pessoais envolvendo, nos termos da lei (art. 5º, inciso X, Lei 13.709/2018), "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".[88]

O capítulo IV da Lei 13.709/2018 é específico quando da ocorrência de "Tratamento de Dados Pessoais pelo Poder Público", definindo, em 10 artigos, as regras e responsabilidades da pessoa jurídica de direito público.[89]

Sabe-se que o Estado detém grande poder em relação aos cidadãos e a organizações, com prerrogativas advindas da supremacia do interesse público. Nesse sentido, a LGPD não se aplicará ao Poder Público para tratamento de dados que envolvam segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, que deverão ser tratados de acordo com legislação específica, a qual deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público.[90]

A relação jurídica estabelecida entre o Poder Público e o indivíduo titular de dados pessoais é marcada pela assimetria de poder, seja em decorrência da natureza jurídica do ente estatal que atua com poder de império, dotado de poderes para a consecução de seus deveres, como pela circunstância objetiva de que o ente estatal detém grande quantidade de dados

---

[85] PINHEIRO. Patrícia Pack – Proteção de Dados Pessoais. Comentários à Lei 13.709/2018.
[86] COTS. Márcio, OLIVEIRA. Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. p. 145.
[87] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 176.
[88] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 490.
[89] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 138.
[90] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 498.

pessoais em seus bancos de dados, como insumo ou subproduto do desempenho de sua atividade.[91]

É inerente à atividade administrativa a gestão de uma série de banco de dados potencialmente sensíveis, sendo que a coleta e tratamento desses dados é um ponto nevrálgico em termos de políticas públicas que tenham escala.[92]

Ora, interesse público e direitos fundamentais precisam caminhar em harmonia, e sempre que o primeiro se distancia do segundo, certamente arbitrariedades e injustiças ganharão maior espaço do desempenho das atividades públicas.[93]

Interessante pontuar que, na dinâmica contemporânea, muito se discute sobre o próprio conceito de interesse público. Em um cenário cada vez mais plural e heterogêneo, com demandas oriundas de diversos grupos identitários, nem sempre relacionados ou convergentes, torna-se complexo identificar o que vocaliza os interesses do Estado ou da coletividade e o que integra mero interesse particular.[94]

3.2.2 - Compartilhamento de Dados pelo Poder Público

O Poder Público poderá realizar tratamento de dados em determinadas circunstâncias, o que inclui a comunicação e compartilhamento de dados com terceiros.[95] Porém, a LGPD estabeleceu regras específicas para tais casos[96], pois é preocupação fundamentada, ante o aumento crescente da importância da informação na economia, que os órgãos públicos, seus dirigentes e funcionalismo, sejam cada vez mais pressionados para transferência de dados à iniciativa privada.[97]

Eventual compartilhamento de informações pessoais de interesse público deve ser expressamente autorizado por lei, com base nos critérios da necessidade, proporcionalidade e adequação, de modo a não tornar o direito fundamental à privacidade inócuo.[98]

3.2.3 - Adequação do Poder Público à LGPD exige Governança Corporativa

A LGPD prevê que os agentes poderão formular regras de boas práticas e de

---

[91] MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. p. 245.
[92] MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. p. 246.
[93] COTS. Márcio, OLIVEIRA. Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. p. 145.
[94] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 139.
[95] Art. 26 da Lei n. 13.709/2018.
[96] Arts. 26 e 27 da Lei n. 13.709/2018.
[97] COTS. Márcio, OLIVEIRA. Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. p. 152.
[98] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 500.

governança[99] que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, considerando a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento.[100]

Nesse contexto, as boas práticas devem ser compreendidas como o conjunto de princípios e ações voltado ao atingimento de metas, desenvolvimento da organização e manutenção da credibilidade do público em relação a tal. Aliada a esta cultura, indispensável a noção de *compliance,* a qual enseja a ideia de estar em conformidade com as leis e os regulamentos internos e externos que envolvem determinada empresa.[101]

O referido programa de governança deverá contar com garantias de acompanhamento periódico e planos de contingência, com vistas a conter eventuais impactos na hipótese de ocorrência de incidentes de segurança, demonstrando o comprometimento do controlador com a adoção de boas práticas no desenvolvimento de seus processos.[102]

A lei brasileira traz ainda a obrigatoriedade da figura do Encarregado pelo Tratamento de Dados Pessoais, cargo similar ao do Data Protection Officer – DPO, da legislação europeia.[103] O art. 41 da LGPD impõe o dever ao controlador de indicar o Encarregado, que pode ser tanto pessoa natural, quanto pessoa jurídica.

A designação do Encarregado deve ocorrer baseada nas qualidades profissionais do indicado, particularmente em seu conhecimento da legislação de proteção de dados, das práticas de tratamento de dados pessoais, e na sua capacidade em cumprir os requisitos da Lei Geral de Proteção de Dados. Quanto mais complexas forem as atividades de tratamento de dados realizadas pela organização, maior deverá ser o nível de conhecimento técnico do Encarregado.[104]

Neste diapasão, surge mais um desafio para o Poder Público, o de encontrar entre seus

---

[99] Art. 50 da Lei n. 13.709/2018.
[100] MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. Edição do Kindle.
[101] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 182.
[102] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 183.
[103]MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. p. 318.
[104] MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. p. 320.

servidores perfil compatível com as premissas exigidas para exercer a função de Encarregado, ou partir para o mercado privado na busca de preencher essa lacuna.

O Poder Público tem realizado o processo de indicação do Encarregado pelo Tratamento de Dados Pessoais, como pode-se observar no Tribunal de Justiça de Santa Catarina - TJSC[105], na Agência Nacional de Telecomunicações - ANATEL[106], na Agência Nacional de Saúde Suplementar - ANS[107] e no Tribunal de Contas do Estado de Rondônia – TCERO.[108] O Tribunal de Justiça de São Paulo – TJSP inovou e instituiu um "Órgão Encarregado de Proteção de Dados Pessoais do Poder Judiciário do Estado de São Paulo", composto por 5 servidores.[109]

3.2.4 - Harmonização entre a LGPD e a Lei de Acesso a Informação

As relações existentes entre o direito à privacidade e o direito à informação têm ocupado posição destacada nos recentes debates jurídicos. O tema comporta análises por distintas perspectivas – sociológica, econômica, centrada na tecnologia da informação, por exemplo. Mesmo quando predominantemente tratado sob o viés jurídico, é possível vislumbrá-las sob a ótica do direito constitucional, do direito administrativo, ou como manifestação de um direito de personalidade.[110] A Lei de Acesso à Informação, entrou em vigor em maio de 2012. Marco muito importante para a Administração Pública brasileira, essa lei regulamentou as informações que são manuseadas pelo poder público.[111]

Ambas as leis (LGPD e LAI) são inspiradas pelo valor da transparência da atividade pública, pelo qual o indivíduo, pessoa natural, tem a possibilidade de exercer a defesa de seus direitos e garantias fundamentais contra o Estado (liberdade negativa) e exercer o efetivo controle da atividade pública (liberdade positiva), como forma de equalizar a relação entre cidadão e Estado, marcada pela assimetria de poder em desfavor do indivíduo.[112]

A Lei de Acesso à Informação, guarda similitudes e divergências com a Lei Geral de Proteção de Dados Pessoais. Cada qual possui diversos fundamentos e matrizes sobre as quais se estruturam. No entanto, esta última acrescenta pontos essenciais, não regulados pela primeira. Ainda que seja relevante a garantia da transparência, igualmente importante é a

[105] TJSC - Portaria nº 1.481, de 17 de julho de 2020.
[106] ANATEL - Portaria nº 1.197, de 25 de agosto de 2020.
[107] ANS - Portaria nº 283, de 10 de agosto de 2020.
[108] TCERO - Portaria nº 189, de 27 de fevereiro de 2020.
[109] TJSP - Portaria nº 9.913, de 4 de setembro de 2020.
[110] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 200.
[111] PINHEIRO. Patrícia Pack. Direito Digital.
[112] MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. p. 247.

tutela dos dados pessoais – principalmente em um cenário globalizado, em que os dados pessoais se tornaram importantes elementos comerciáveis.[113]

Mister se faz, portanto, que se observe a difícil tarefa do Poder Público em se aplicar a harmonização entre os institutos, de acordo com o caso concreto, sem comprometer os preceitos basilares de ambos, quais sejam o direito à informação e o direito à privacidade.

3.2.5 - Da Responsabilidade e Sanções Previstas na LGPD

Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.[114]

Conforme aponta Celso Antônio Bandeira de Mello, os órgãos públicos estão no âmbito do regime administrativo, logo estão sujeitos às normas e aos parâmetros deste, e consequentemente respondem administrativa e não judicialmente, daí a necessidade de tratamento específico dentro dos limites das normas administrativas.[115]

Dito isso, o art. 31 permite que, em caso de violação ao disposto na LGPD, a Autoridade Nacional de Proteção de Dados remeta informe aos órgãos públicos responsáveis pelo tratamento, com a indicação das medidas a serem tomadas para fazer cessar a infração.[116]

Não resta dúvida de que o ato de informar as medidas cabíveis para cessação da violação de direitos e garantias fundamentais decorrentes do tratamento de dados pessoais pelo Poder Público não retira ou mitiga o poder sancionatório da autoridade nacional.[117]

Quanto às sanções previstas na LGPD, o capítulo VIII é voltado ao processo de fiscalização do cumprimento das regras de tratamento e proteção de dados pessoais, conforme dispostas pelo texto legal. A competência fiscalizatória e sancionatória incumbe majoritariamente à Autoridade Nacional de Proteção de Dados, porém sem excluir o eventual cabimento de demais ações administrativas, civis ou penais aplicáveis a cada caso.[118]

As sanções administrativas a que estão sujeitos os agentes de tratamento de dados, são previstas no artigo 52 que prevê a aplicação de advertência, multa e bloqueio dos dados

---

[113] TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. p. 216.
[114] Art. 31 da Lei n. 13.709/2018.
[115] PINHEIRO. Patrícia Peck. Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD. p. 1024-1025. Edição do Kindle.
[116] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 145.
[117] MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. LGPD – Lei Geral de Proteção de Dados Comentada. p. 288.
[118] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. p. 187.

pessoais, entre outros.

Partindo dessa premissa, entende-se que a imputação de sanções deve sempre observar o princípio constitucional da proporcionalidade como um critério para prevenir e inibir possíveis abusos do poder estatal quando do exercício de suas funções.

Como a regulação dos dados pessoais será efetuada por uma agência nacional, a aplicação das sanções deve seguir os mesmos nortes e princípios do direito administrativo.[119]

A obrigação imposta tem que ser muito bem descrita, a fim de não haver dúvidas quanto à obrigação de fazer ou de não fazer, pois é sobre esse tipo de obrigação que a multa diária faz sentido.[120]

Desta forma, conclui-se que infringir a LGPD sujeita o Poder Público, e, consequentemente, o agente público, às sanções previstas no referido ordenamento, não obstante a cominação com outras ações administrativas, civis ou penais.

CONSIDERAÇÕES FINAIS

A busca por conformidade à Lei Geral de Proteção de Dados Pessoais, como vimos, é sem dúvida um grande desafio para as organizações, em especial para o Poder Público, que via de regra, detém grande volume de dados pessoais sob sua custódia e é inerente a suas atividades o tratamento de dados.

O cenário ao qual está inserida a partir da vigência da LGPD é complexo e "estar em conformidade" decorre de inúmeros fatores, quais sejam humanos, tecnológicos, normativos, entre outros. Desta forma, para se promover a utilização de medidas 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 difusão, conforme preconizado na referida Lei, a organização precisa entender sua conjuntura atual, e principalmente, os desafios e os possíveis impactos no negócio.

Assim, se faz necessário que o Poder Público utilize da aplicação de boas práticas e de governança em privacidade, abrangendo investimentos em capital humano especializado (encarregado pelo tratamento de dados pessoais - DPO), em ferramentas de segurança (software e hardware), na melhoria de procedimentos e fluxos internos e externos (estrutura organizacional), bem como, na implementação de uma cultura organizacional (treinamentos e

[119] PINHEIRO. Patrícia Peck. Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD. p. 1302-1305. Edição do Kindle.
[120] COTS. Márcio, OLIVEIRA. Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. p. 219.

conscientização) voltada para o tema, e ainda, devem ser criados mecanismos no nível do plano tático (políticas de segurança) de forma a dar as diretrizes para as atividades requeridas no nível operacional, que é onde ocorrem os incidentes de segurança. Desta forma, a Administração Pública estará preparada para enfrentar os desafios e questões relacionadas à proteção e salvaguarda das informações pessoais sob sua tutela.

Nada obstante, é possível afirmar que, sem gestão de segurança da informação e privacidade de dados, certamente, não haverá sequer uma organização pública ou privada em *compliance* com a Lei Geral de Proteção de Dados Pessoais.

Percebe-se que todo o contexto de busca por conformidade à Lei está intrinsicamente relacionado com a segurança da informação, e, é através dela, que o Poder Público deve construir o alicerce para implementar os controles, políticas, processos, procedimentos e estrutura organizacional, que uma vez estabelecidos, devem ser monitorados, analisados criticamente e melhorados, quando necessário, para manter o nível adequado de proteção dos dados pessoais contra ameaças, vulnerabilidades, riscos e ataques, garantindo assim, a tríade confidencialidade, integridade e disponibilidade dos dados.

Neste diapasão, um fator preponderante para o sucesso das ações emanadas pelo Poder Público perante o titular de dados pessoais, é a aplicação do princípio da transparência ao realizar o tratamento de dados, devendo, via de regra, se amparar em sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legalísticas do serviço público.

Desta maneira, o Poder Público deve procurar harmonizar o cumprimento à LGPD com outros institutos legais como forma de equalizar a relação entre os direitos, buscando a proteção dos preceitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (titular dos dados), mitigando assim, possíveis sanções administrativas, civis e penais.

REFERÊNCIAS DAS FONTES CITADAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 27002 – **Tecnologia da Informação - Código de Prática para a Gestão de Segurança da Informação –** 2013.

BAARS, Hans – HINTZBERGEN, Kees - HINTZBERGEN, Juli – SMULDERS, André. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. BRASPORT; Edição: 1. 2018.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**. Forense; Edição: 2. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: encurtador.com.br/kqrU3. Acesso em: 16/04/2020.

BRASIL. **Decreto Nº 9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 06/12/2020.

BRASIL. **Lei Nº 12.527, de 18 de novembro de 2011.** Lei de Acesso a Informação. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 06/12/2020.

BRASIL. **Lei Nº 13.709, de 14 de agosto de 2018.** 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: 06/12/2020.

BRASIL. **Lei Nº 14.010, de 10 de junho de 2020.** 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: 06/12/2020.

COELHO, Flavia Estélia Silva. **Gestão da Segurança da Informação - NBR 27001 e NBR 27002**. Rio de Janeiro: RNP/ESR, 2014.

COSTA, Marcelo Antonio Sampaio Lemos. **Computação Forense: A análise forense no contexto da resposta a incidentes computacionais**. Campinas, SP: Millennium Editora; Edição: 3, 2011.

COTS. Márcio, OLIVEIRA. Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. 3. ed. ver., atual e ampl. São Paulo: Thomson Reuters Brasil, 2019.

DELLA VECCHIA, Evandro. **Perícia Digital: Da Investigação à Análise Forense**. Campinas, SP: Millennium, 2014.

FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018.** São Paulo: Thomson Reuters Brasil, 2019.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. BRASPORT; Edição: 1. 2012.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

MALDONADO, Viviane Nóbrega - BLUM, Renato Opice. **LGPD – Lei Geral de Proteção de Dados Comentada**. Thomson Reuters Revista dos Tribunais; Edição: 1. 2019.

MALDONADO, Viviane Nóbrega. **LGPD: Lei Geral de Proteção de Dados Pessoais: Manual de Implementação**. São Paulo: Thomson Reuters Brasil, 2019.

PINHEIRO, Patricia Peck. **Direito Digital**. Saraiva; 5ª Edição. 2013.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018 (LGPD)**. Saraiva; 1ª Edição. 2018.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva**. Rio de Janeiro: Elsevier; 2ª Edição, 2014.

TEPEDINO, Gustavo – FRAZÃO, Ana – OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** Revista dos Tribunais. 2ª Tiragem. 2019.