2023

PPGD
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO • UNIRIO

REVISTA DIREITO DAS POLÍTICAS PÚBLICAS

Law and Public Policy Review

ISSN 2675-1143

Volume 5, n. 1
Janeiro - Junho

Qualis B2

UNIRIO
Universidade Federal do Estado do Rio de Janeiro

Revista do Programa de Pós-Graduação em Direito da Universidade Federal do Estado do Rio de Janeiro (UNIRIO)

http://seer.unirio.br/rdpp/index
rdpp@unirio.br

REVISTA DIREITO DAS POLÍTICAS PÚBLICAS

LAW AND PUBLIC POLICY REVIEW

VOLUME N.º 5 – NÚMERO 1

ISSN 2675-1143

Rio de Janeiro, 2023

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

Os programas de *compliance* e governança nas empresas conformidade entre políticas de segurança da informação e a LGPD

Compliance and governance programs in companies

Compliance between information security policies and LGPD

Liliana Bastos Pereira Santo de Azevedo Rodrigues[17]
Universidade Federal do Rio Grande do Norte. Professora. Advogada. Natal (RN). Brasil
Calígena Batista de Paiva Silva[18]
Universidade Federal do Rio Grande do Norte. Graduanda em Direito. Natal (RN). Brasil

RESUMO
O presente trabalho tem por objeto articular os requisitos de conformidade das organizações empresariais decorrentes da Lei Geral de Proteção de Dados com os benefícios de sua estruturação no âmbito de um Programa de *Compliance* e Governança Corporativa. Assim, o objetivo geral da pesquisa é apresentar como a LGPD, as Políticas de Segurança da Informação e os programas de *Compliance* e Governança podem interagir para proporcionar uma melhor adequação das empresas às regras estabelecidas pela legislação de proteção de dados. Trata-se de uma pesquisa de abordagem qualitativa, onde foram consultadas bibliografias de referência. O artigo está estruturado com três seções de desenvolvimento, abordando os temas Lei Geral de Proteção de Dados, Políticas de Segurança da Informação e *Compliance* e Governança dentro da organização, tudo com o fim de demonstrar a importância do cumprimento das regras estabelecidas pela legislação externa e normativos internos quanto à segurança da informação.

ABSTRACT
The purpose of this work is to articulate the compliance requirements of business organizations arising from the General Data Protection Law with the benefits of structuring it within the scope of a Compliance and Corporate Governance Program. Thus, the general objective of the research is to present how the LGPD, the Information Security Policies and the Compliance and Governance programs can interact to provide a better adaptation of companies to the rules established by the data protection legislation. This is a research with a qualitative approach, where selected bibliographies were consulted. The article is structured with three development sections, addressing the General Data Protection Law, Information Security Policies and Compliance and Governance within the organization, all with the aim of demonstrating the importance of complying with the rules established by external legislation and internal regulations regarding information security.

[17] Lattes: http://lattes.cnpq.br/3256952255730615
[18] Lattes: http://lattes.cnpq.br/1214596802953906

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

PALAVRAS-CHAVE:
Compliance; Governança; Segurança da Informação; Lei Geral de Proteção de Dados; LGPD.

KEYWORDS:
Compliance; Governance; Information Security; General Data Protection Law; GDPL.

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

1. INTRODUÇÃO

No Brasil, em 14 de agosto de 2018, foi sancionada a Lei Federal nº 13.709, conhecida como Lei Geral de Proteção de Dados - LGPD, que entrou totalmente em vigor em agosto de 2020, após vinte e quatro meses de sua publicação. A LGPD, de acordo com seu primeiro artigo, 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 (Brasil, 2018).

Desse modo, a Lei foi desenvolvida buscando a proteção dos direitos de liberdade e privacidade e, ainda, o livre desenvolvimento da personalidade da pessoa natural, aplicando-se a qualquer pessoa, seja ela física ou jurídica, que atue no direito público ou privado, realizando o tratamento de dados pessoais de pessoas naturais, para fins comerciais. A Lei é voltada para o titular dos dados pessoais, definido, em seu art. 5º, inciso V, como a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Brasil, 2018). Portanto, ela não se aplica aos dados de pessoas jurídicas e não confere proteção a eles.

Podemos enumerar algumas vantagens da legislação. Por parte dos titulares dos dados, uma maior segurança e emancipação sobre a coleta e o tratamento dos seus dados pessoais. Esse fato traz mais transparência com relação ao tratamento realizado com as informações, conferindo também mais conhecimento sobre o processo realizado pelas empresas que fazem a coleta dos dados para a execução dos seus objetivos comerciais.

Já para as empresas, o fato de o titular ter maior transparência sobre os processos realizados com seus dados, pode trazer uma responsabilidade ética maior na execução de seus processos de segurança, podendo levar a empresa a se destacar por seus níveis de segurança da informação e governança.

Assim, considera-se a existência de uma Política de Segurança da Informação - PSI, um documento que reúne regras, práticas, diretrizes e procedimentos acerca da segurança da informação na empresa e que tem como objetivo a minimização de riscos de violação ou perdas, protegendo as informações da empresa de possíveis causadores de danos, sejam eles intencionais ou não.

O presente trabalho tem como objetivo geral apresentar como a LGPD, as Políticas de Segurança da Informação e os programas de *Compliance* e Governança podem interagir para

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

proporcionar uma melhor adequação das empresas às regras estabelecidas pela legislação de proteção de dados.

Quanto aos objetivos específicos, a pesquisa busca: i) trazer informações sobre a Lei Geral de Proteção de Dados, quanto a sua relevância para a segurança de dados pessoais dos indivíduos; ii) expor a importância da implementação de Políticas de Segurança da Informação nas empresas para melhor gerenciamento de dados sensíveis, buscando evitar possíveis crimes digitais, prezando pela privacidade e segurança digital da pessoa natural titular dos dados; e, por fim, iii) indicar como o *Compliance* e a Governança podem auxiliar no cumprimento das normas e regras estabelecidas pela legislação e pela PSI.

A metodologia aplicada para elaboração do trabalho traz à tona uma pesquisa de abordagem qualitativa, onde foram consultadas bibliografias visando trazer conceitos e informações fundamentadas acerca dos temas a serem discutidos.

Com relação à estrutura, o trabalho foi dividido em três momentos. No primeiro, apresenta-se uma análise da Lei Geral de Proteção de Dados – LGPD, onde se pontuam informações sobre a sua relevância e requisitos para o cumprimento de suas normas.

Partindo desse ponto, no segundo momento, é explicada a pertinência da elaboração e aplicação de Políticas de Segurança da Informação – PSI dentro das organizações, mostrando como elas podem servir no contexto empresarial, diante das normas trazidas pela LGPD.

E, por fim, no terceiro momento é levantada a importância da existência de um setor de *Compliance* e Governança dentro da organização, para que se possa estimular e regulamentar o cumprimento das regras estabelecidas pela legislação externa e normativas internas, tanto com relação à aplicação das regras, quanto pelo monitoramento das ações executadas.

2. LEI GERAL DE PROTEÇÃO DE DADOS: ALGUNS ASPECTOS

A Lei Geral de Proteção de Dados – LGPD foi sancionada no Brasil em 2018 e trouxe com ela diversas diretrizes a serem seguidas pelas empresas, para que estejam de acordo com os mandamentos constitucionais. Trata-se de um marco legal que confere proteção aos cidadãos, que são as pessoas naturais, contra o uso de seus dados ou informações de maneira irregular.

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

Tal norma foi inspirada na regulação europeia de proteção de dados, General Data Protection Regulation – GDPR, que entrou em debate na União Europeia - UE e foi aprovada em 2016. A GDPR tem como objetivo abordar a proteção da privacidade das pessoas físicas, no que diz respeito ao tratamento de dados pessoais, para que seja conferida mais transparência, controle e segurança com relação aos dados armazenados pelas companhias.

Ao sancionar tal regulação, a UE fez com que outros países também tivessem a iniciativa de desenvolver uma legislação de mesmo nível. Isso ocorreu porque "o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE" (Pinheiro, 2020, p. 4).

Inicialmente, a LGPD teve um veto presidencial com relação à criação da Autoridade Nacional de Proteção de Dados Pessoais – ANPD, que geraria o não reconhecimento da LGPD pela UE como legislação de mesmo nível, pois uma de suas exigências seria a existência de uma autoridade nacional de fiscalização independente. Tal veto, porém, foi alterado pela Medida Provisória nº 869 de 2018 e, com isso, foi criada a ANPD. A MP nº 869/2018 foi transformada em lei pela aprovação da Lei nº 13.853 de 2019, que dispõe sobre a proteção de dados pessoais e cria a ANPD, proporcionando mais segurança e estabilidade para a LGPD.

A ANPD tem competências normativas, deliberativas, fiscalizadoras e sancionatórias, sendo a sua principal função "zelar pela proteção de dados pessoais, nos termos da legislação" (art. 55-J, I). Trata-se de um órgão da administração pública de autoridade nacional responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território brasileiro.

Como dito anteriormente, a legislação de proteção de dados estabelece como titular apenas a pessoa natural a quem se referem os dados pessoais que serão objeto de tratamento. Assim, a lei visa proteger somente os dados de pessoas físicas, não conferindo proteção aos dados de pessoas jurídicas. Porém, o controlador ou o operador, que serão os responsáveis por decidir e realizar o tratamento dos dados pessoais, podem ser tanto pessoa natural quanto jurídica, de direito público ou privado.

Os dados pessoais são definidos como toda informação relacionada a uma pessoa identificada ou identificável, podendo alcançar inclusive localização, placas de automóveis, perfis de compras, números de Internet Protocol - IP, dados acadêmicos, entre outros, não se limitando apenas a informações como nome, sobrenome, endereço, etc. (Pinheiro, 2020).

Já o tratamento dos dados é definido pela LGPD, em seu art. 5º, X, como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção,

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Para que seja realizado o tratamento dos Dados Pessoais, é estabelecido que deve haver o consentimento do titular, por meio de documento escrito ou de algum outro modo, desde que seja demonstrada a manifestação de vontade do titular. Além disso, em seu art. 6º, a lei dispõe que se deve ainda observar a boa-fé e princípios como:

> I - finalidade: realização do tratamento para propósitos legítimos […];
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades […];
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade […];
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade […];
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e […] agentes […];
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados [...];
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Brasil, 2018)

Assim, entende-se que as organizações deverão utilizar os dados apenas para fins legítimos, adequando e limitando o tratamento dos dados de acordo com sua finalidade, não ultrapassando os limites necessários e garantindo aos titulares o livre acesso sobre a maneira e a duração da realização do tratamento.

Devem ser garantidas ainda aos titulares: exatidão, clareza, relevância e atualização dos dados, proporcionando-lhes informações claras, precisas e acessíveis sobre o procedimento e sobre quem (qual agente) irá realizá-lo; além disso, a segurança dos dados deve ser imprescindivelmente garantida através de medidas técnicas e administrativas, bem como a adoção de medidas para prevenir possíveis danos.

A Lei impõe ainda que não devem ser utilizados os dados pessoais dos indivíduos para fins discriminatórios, ilícitos ou abusivos; e também que deve haver a demonstração de que foram adotadas medidas eficazes e capazes de comprovar que as normas de proteção dos dados foram cumpridas.

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

São levantadas as hipóteses em que o tratamento de dados pode ser realizado de forma lícita e entre elas está o tratamento para fins de estudos e realização de pesquisa. Nesses casos, para que possam ser utilizados os dados, a LGPD aponta que, sempre que possível, deve ser realizada a sua anonimização, que, como definido por Pinheiro (2020), se trata da possibilidade de não identificação do titular. E, quando se tratar de um tratamento de dados de acesso público, deve ser considerada a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização.

Em caso de dados que sejam tornados públicos pelo titular deles, resguardados seus direitos de titular e os princípios citados anteriormente, se dispensa a exigência de consentimento para a realização de tratamento dos dados. Desse modo, os agentes que irão realizar o tratamento não se isentam das demais obrigações previstas pela LGPD que versam sobre a proteção dos direitos do titular e princípios gerais.

Com relação ao Tratamento de Dados Pessoais Sensíveis, que são os dados 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, a Lei traz algumas restrições, como a necessidade de consentimento do titular ou seu responsável legal, de forma específica e destacada, apenas para determinadas finalidades.

Além disso, os Dados Pessoais Sensíveis podem ser tratados sem consentimento nos casos em que for indispensável a sua realização para cumprimento de obrigação legal ou regulatória pelo controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei de Arbitragem (nº 9.307/96); proteção da vida ou da incolumidade física do titular ou de terceiro; tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (art. 11, II).

Regulamentação especial também é dada com relação ao tratamento de Dados Pessoais de Crianças e Adolescentes, que deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (esse consentimento deve

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

ser verificado pelo controlador). Os dados poderão ser coletados sem o consentimento referido anteriormente, quando a coleta for necessária para contatar os pais ou o responsável legal, devendo ser utilizados uma única vez e sem armazenamento, ou para sua proteção, e não poderão ser repassados a terceiros, em hipótese alguma, sem o consentimento já tratado no trecho anterior.

Sobre as possibilidades de término do tratamento de dados pessoais, a LGPD traz as hipóteses de verificação de alcance da finalidade do uso dos dados, ou de que estes deixaram de ser necessários/pertinentes para alcançá-la; fim do período de tratamento; a revogação do consentimento expressa pelo titular; ou ainda por determinação da autoridade nacional, em caso de violação das disposições expressas na legislação em questão.

Os dados que estavam sendo utilizados para tratamento, após o seu término, deverão ser eliminados, exceto quando deva ser realizado:

> Art, 16 [...] - I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (Brasil, 2018).

Violadas as normas estabelecidas, a legislação traz a responsabilização dos agentes, sejam eles órgãos públicos ou mesmo o controlador e o operador. Quando se tratar de órgão público, a autoridade nacional, como estabelecido no art. 31 da LGPD, poderá enviar informe contendo as medidas cabíveis para que a violação cesse, podendo também sugerir a adoção de padrões e de boas práticas para a execução dos tratamentos de dados pessoais pelo Poder Público.

Já com relação a violações da LGPD em razão do exercício da atividade de tratamento de dados, realizadas pelo controlador ou operador, caso estes venham a causar dano patrimonial, moral, individual ou coletivo, serão obrigados a repará-lo.

Para isto, a Lei estabelece que (art. 42, §1º, I e II) o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, sendo a ele equiparado; e que os controladores que estiverem diretamente envolvidos no tratamento, do qual decorreram danos ao titular dos dados, respondem solidariamente.

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

Conforme o art. 43 da LGPD, a responsabilização dos agentes de tratamento deixa de ser aplicada somente se for provado que eles não realizaram o tratamento de dados pessoais que lhes é atribuído; que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Considera-se irregular o tratamento que fuja ao padrão de segurança que o titular dos dados pode esperar e ao cumprimento do que diz a legislação. Pois é estabelecido que o controlador tem o dever de adotar medidas de segurança, técnicas e também administrativas, que sejam aptas a proteger os dados pessoais dos titulares de possíveis acessos não autorizados ou ainda situações acidentais ou ilícitas que causem destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Caso alguma situação das citadas no parágrafo anterior venha a ocorrer, deve ser feita a comunicação, pelo controlador, à autoridade nacional e ao titular, descrevendo a situação, os dados e medidas cabíveis, além de mencionar os possíveis riscos relacionados ao incidente. E, além disso, a estrutura dos sistemas utilizados para realizar o tratamento dos dados deve atender todos os requisitos de segurança, padrões de boas práticas e de governança, bem como aos princípios previstos na LGPD e demais normas que tragam regulamentações.

As penalidades previstas com relação às infrações cometidas contra o estabelecido na LGPD foram adaptadas ao contexto e realidade social e econômica do Brasil. Assim, devem ser respeitados alguns requisitos como o da proporcionalidade entre a gravidade da falta e a intensidade da sanção, critérios como a observação da gravidade e natureza das infrações, o impacto do incidente e quais dados ele afeta.

Além disso, deve ainda ser observado se existe boa-fé por parte da empresa no tratamento dos dados; o que motivou a empresa a tratar os dados/que vantagem era pretendida; o poder econômico da empresa; se há reincidência; qual o dano gerado; cooperação do infrator; o desenvolvimento e aplicação de medidas tecnológicas e organizacionais que auxiliem na prevenção/minimização do dano; bem como a adoção de políticas de boas práticas e governança e também de medidas corretivas.

As sanções previstas na LGPD variam entre advertência, com prazo para adoção de medidas corretivas; multa, limitada ao total de R$ 50.000.000,00 por infração; multa diária, também limitada a esse valor; divulgação da infração ao público, após ser devidamente constatada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração (por até seis meses, prorrogável por igual período); suspensão temporária do tratamento de dados pessoais a que se refere a infração (por até seis meses, prorrogável por igual período); e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Assim, para uma melhor execução do tratamento de dados pessoais, a LGPD estabelece que os controladores e operadores poderão formular regras de boas práticas e governança com relação às condições de organização, o regime de funcionamento, as normas de segurança, as obrigações específicas para os envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e mitigação de riscos, entre outros aspectos relacionados ao tratamento de dados pessoais.

Daí a importância de elaborar uma PSI adequada e também da instauração de um Programa de *Compliance* e Governança, fazendo-se fundamentais para guiar e fomentar os procedimentos citados anteriormente.

3. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

No cenário atual, onde cada vez mais as tecnologias estão se desenvolvendo, vemos a busca das empresas por uma adequação aos recursos que podem facilitar seu crescimento. Desse modo, grande parte delas possui seus dados armazenados digitalmente, o que traz a necessidade de uma ferramenta para garantir a segurança desses dados/informações. Para isso, a implementação de uma Política de Segurança da Informação – PSI seria o mais adequado.

As Políticas de Segurança da Informação tratam-se de mecanismos preventivos de proteção de dados e processos importantes de uma organização que definem um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos (Dias, 2000 apud Laureano, 2005, p. 56).

Assim, uma PSI busca garantir a proteção das informações corporativas contra possíveis ameaças que possam prejudicar a organização. Ela previne danos ao andamento do negócio e padroniza procedimentos. Isto porque a PSI deve estabelecer princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos computacionais e, consequentemente, as informações por eles manipuladas. É importante que a política estabeleça

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

ainda as responsabilidades das funções relacionadas com a segurança e discrimine as principais ameaças, riscos e impactos envolvidos (Dias, 2000, apud Laureano, 2005, p. 56).

Laureano (2005) destaca ainda que essas políticas devem ir além dos aspectos relacionados apenas com os sistemas de informação e recursos computacionais, devendo também estar integradas com as políticas institucionais, planejamento estratégico e metas da empresa.

Em um contexto nacional, há sempre legislações que devem ser seguidas para que o desenvolvimento do país se dê de modo a garantir o melhor para todos os indivíduos. Nesse mesmo padrão, as políticas de segurança vêm para definir os padrões que devem ser seguidos pelas empresas para que estas se desenvolvam plenamente.

A norma que serve como base para a criação das PSI é a ISO (International Organization for Standardization) 27002, que traz em sua estrutura medidas de segurança sobre controles organizacionais, controle de pessoas, controles físicos e controles tecnológicos.

De acordo com Fontes (2012, p. 23), esta norma "define um código de prática para gestão de segurança da informação e orienta quais elementos devem ser considerados para uma adequada proteção da informação".

Para realizar a implementação de uma PSI, em primeiro lugar, é necessário fazer um diagnóstico sobre as informações da empresa, para que se possa saber quais dados devem ser protegidos. Desse modo, poderão ser identificadas também as principais ameaças e fragilidades com relação à organização, o que vai garantir uma PSI com mais efetividade.

Assim, é normatizado que as informações utilizadas nas organizações devem ser protegidas seguindo alguns requisitos/princípios, são eles: confidencialidade, integridade e disponibilidade (Fontes, 2012, p. 04).

A confidencialidade garante que apenas pessoas previamente autorizadas poderão acessar as informações guardadas; a integridade busca manter a legitimidade da informação, garantindo que ela não seja modificada ou eliminada sem autorização; e a disponibilidade garante que os dados e sistemas estejam disponíveis para pessoas autorizadas no momento em que se tornar necessário (Lento; Silva; Lung, 2006).

Qualquer falha nesses princípios pode acarretar impactos negativos para a organização, pois eles certificam que todos os aspectos importantes sejam observados atentamente, portanto é necessário garantir na PSI que todos estes requisitos sejam efetivamente cumpridos.

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

Além do diagnóstico da empresa, para a implementação da PSI, são necessários mecanismos de segurança que possibilitem a adoção de controles. Tais mecanismos são responsáveis pela concretização das políticas de segurança nos sistemas computacionais. Dessa forma, as políticas de segurança, cujos comportamentos que recomendam são expressos por meio de modelos de segurança, são implantadas por mecanismos de segurança da informação. Tais mecanismos exercem os controles (físicos e/ou lógicos) necessários para garantir que as propriedades de segurança (confidencialidade, integridade e disponibilidade) sejam mantidas em conformidade com as necessidades do negócio (Lento; Silva; Lung, 2006, apud Hummes, 2017).

Assim, os mecanismos de segurança trazem os controles que irão nortear e manter a aplicação dos três princípios da segurança da informação citados anteriormente (confidencialidade, integridade e disponibilidade). A segurança da informação traz em seu rol a avaliação de riscos à infraestrutura da tecnologia da informação da empresa, visando protegê-la de possíveis ataques que objetivem roubar dados privados e ainda contra outras ameaças digitais, como vírus.

Com isso em vista, a PSI oficializa as diretrizes que irão guiar os procedimentos a serem seguidos para garantir o bom funcionamento da segurança da informação, assegurando que sejam seguidos ao longo do tempo, protegendo e assegurando a integridade dos dados.

O diagnóstico realizado na empresa abre espaço para o planejamento da PSI, onde se recomenda que haja o máximo de representação na equipe responsável por sua elaboração, visto que essa política irá afetar todos os setores da empresa. Desse modo, frisa-se que devem ser considerados os aspectos de todas as áreas possíveis nesse desenvolvimento, para que as normas não deixem de ser seguidas em algum momento, por não estarem de acordo com as atividades realizadas em determinado setor.

Após o diagnóstico da empresa, o planejamento e elaboração da PSI, deve ser realizada a sua implementação. Porém, isto não quer dizer que o processo esteja finalizado. Pois, para que a PSI seja efetiva, precisa ser revisada, com o propósito de realizar o acompanhamento de suas contribuições, analisando também suas falhas, adequando-as aos padrões da LGPD.

Portanto, é essencial que cada colaborador esteja a par dos riscos e consequências que podem ser acarretados se a proteção dos dados for negligenciada, pois novas ameaças surgem diariamente e, por isso, a segurança nunca deve ser vista como algo finalizado. Assim, mesmo seguindo todos os princípios das PSI, faz-se necessário o seu monitoramento.

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

O monitoramento da efetividade da PSI pode ser feito através de um programa de *Compliance* e Governança que, como será exposto a seguir, se faz responsável pelo cumprimento de normas, pela supervisão e controle das empresas, entre outras atribuições.

4. COMO O *COMPLIANCE* E A GOVERNANÇA AUXILIAM AS EMPRESAS NA IMPLEMENTAÇÃO DAS PSI CONFORME A LGPD

É importante destacar que para uma empresa estar em conformidade com as normas por ela estabelecidas e também com a PSI desenvolvida, a orientação proporcionada pelos programas de *Compliance* e Governança faz-se instrumento primordial.

Isso porque o *Compliance* visa o cumprimento das normas legais e regulamentares das empresas, bem como suas políticas e diretrizes, para evitar, identificar e também solucionar as situações de inconformidade que possam ocorrer, tratando-se de uma estratégia utilizada para alcançar os fins institucionais das organizações. Já a Governança, de acordo com Instituto Brasileiro de Governança Corporativa (IBGC), "é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas".

A existência de um setor de *Compliance* e Governança dentro das empresas é fundamental, independente da necessidade do monitoramento da implementação de Políticas de Segurança da Informação. Pois os programas de *Compliance* "estão inseridos em um contexto de reestruturação estratégica, organizacional e tecnológica, na construção de uma imagem empresarial forte perante clientes e fornecedores, visando a proteção dos valores e da reputação corporativas" (Abbi, 2004, apud Santos, 2018).

Desse modo, no ambiente corporativo, os programas de *Compliance* e Governança irão prezar pela conformidade e integridade da organização, a fim de manter o compromisso com as regras institucionais, dirigindo, monitorando e incentivando os processos que são realizados na empresa, identificando e solucionando situações de inconformidade.

Santos (2018) aponta que quanto maior o volume de recursos envolvidos em projetos e negócios, maior é a probabilidade de práticas de corrupção. Daí a importância de elaborar boas políticas e diretrizes empresariais e sempre prezar pelo seu cumprimento, principalmente

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

com relação ao tratamento de dados sensíveis, como destacado pela Lei Geral de Proteção de Dados – LGPD.

A proteção dos direitos de liberdade e privacidade promovidos pela LGPD, onde a segurança sobre a coleta e tratamento dos dados dos titulares é trazida com maior transparência sobre os processos realizados, traz a exigência de uma maior ética por parte das empresas com relação aos seus processos de segurança. Consequentemente, faz-se necessária a elaboração de uma PSI, objetivando a minimização de riscos de perdas, violação e possíveis danos às informações.

Com a formulação da PSI, como exposto no decorrer deste trabalho, as empresas terão um documento próprio e elaborado para atender especificamente suas necessidades, onde estarão presentes as regras, práticas, diretrizes e procedimentos sobre como deve ser tratada a segurança da informação no ambiente corporativo.

Deste modo, promovendo a implementação de programas de *Compliance* e Governança as empresas estarão respaldadas, para que encontrem mais segurança em sua atuação no mercado, seguindo sua PSI adequadamente e, em caso de surgimento de riscos que possam trazer danos ao objetivo da organização, possam gerenciar os riscos de forma eficaz, buscando a melhor solução para eles, visto que há monitoramento constante.

Essa atuação irá proporcionar ainda a proteção à imagem da empresa, resguardando-a de exposições desnecessárias a riscos que podem ser evitados e controlados, prevenindo prejuízos dentro e fora da instituição. Conforme destacado por Santos (2018, p. 268), um dos benefícios da implementação desses sistemas é justamente o impacto positivo na imagem da empresa perante a sociedade que "advém da boa reputação frente à opinião pública e aos meios de comunicação pelo simples fato de existir um sistema formal de combate à corrupção na empresa".

Portanto, há benefícios variados para as empresas ao estarem em conformidade com a LGPD. Estes benefícios podem ser tanto com relação ao bom funcionamento da empresa, relações interpessoais, com funcionários e clientes, como de natureza econômica, visto que a imagem da empresa em geral reflete em suas ações no mercado e perante o atual cenário de desenvolvimento financeiro.

Revista Direito das Políticas Públicas, vol. 5, n. 1, jan./jun. 2023. ISSN 2675-1143

5. CONSIDERAÇÕES FINAIS

Os dados são utilizados das mais diversas formas. Alguns dados são de carácter público, outros, contêm informações sensíveis e por esse motivo deverão ser protegidos. As empresas necessitam desses dados para exercer as suas funções. Significa dizer, que a sociedade fica vulnerável em relação às informações de carácter sensível que deverão ser protegidas e guardadas em caráter sigiloso.

A LGPD é de fundamental importância para os titulares dos dados que são tratados pelas empresas, buscando sua proteção e ainda trazendo a responsabilização dos agentes em caso de violação das normas. Não basta apenas proteger o titular dos dados, mas ainda informar como esses dados deverão ser trabalhados: desde a sua coleta, à forma de armazenamento, ao seu compartilhamento e tratamento de uma forma geral. Por fim, caso esses procedimentos não sejam verificados, a Lei aplica as consequências jurídicas.

A implementação de PSI nas empresas traz a possibilidade de realizar um melhor tratamento e gerenciamento de dados, em especial os dados sensíveis, para evitar crimes e trazer segurança digital para a pessoa natural titular dos dados.

Assim, espera-se com as informações expostas no decorrer do trabalho, fazer compreender a importância da relação entre estar em conformidade com a LGPD e a implementação da PSI e os Programas de *Compliance* e Governança, visto que eles estão intimamente ligados. O bom funcionamento de uma PSI pode ser feito através dos Programas de *Compliance* e Governança, que irão auxiliar no cumprimento das normas e regras estabelecidas na LGPD e na PSI da instituição, conforme apontado nas informações aqui apresentadas.

6. REFERÊNCIAS

ABNT. NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – *Código de prática para a gestão da segurança da informação*. Rio de Janeiro, 2005.

BRASIL, *Lei Federal n.º 13.709, de 14 de agosto de 2018*. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 7 mar 2023.

DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação.* Axcel Books. Rio de Janeiro, 2000.

FONTES, Edison. *Políticas e Normas para segurança da informação.* Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

IBGC. *Governança Corporativa.* Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 3 abr 2023.

LAUREANO, Marcos Aurelio Pchek. *Gestão de Segurança da Informação.* 2005. Disponível em: www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 22 fev 2023.

LENTO, Luiz Otávio Botelho; DA SILVA FRAGA, Joni; LUNG, Lau Cheuk. A nova geração de modelos de controle de acesso em sistemas computacionais. *Sociedade Brasileira de Computação*, 2006.

PINHEIRO, Patricia Peck. *Proteção de Dados Pessoais:* Comentários à Lei n. 13.709/2018-LGPD. São Paulo: Saraiva Educação, 2020.

SANTOS, Diogo de Almeida Viana dos. Compliance e Legislação Anti-corrupção: Uma perspectiva comparada. *Revista Brasileira de Filosofia do Direito*, Salvador, v. 4, ed. 1, p. 260-281, 2018.

Sobre as autoras:

Liliana Bastos Pereira Santo de Azevedo Rodrigues | E-mail: lisanto@hotmail.com
Consultora e Mentora em Compliance, Presidente e Fundadora da Educompliance, Professora Universitária e Advogada (Brasil-OAB/RN 12.777 e Portugal 52.461P). Associada no escritório Melo e Araújo Sociedade de Advogados, responsável pelos serviços de assessoria, consultoria e certificação em compliance. Bolsista de Pesquisa e Inovação da FAPERN no Instituto de Gestão de Águas do Estado do Rio Grande do Norte - IGARN. Aluna especial do Doutorado em Educação na Universidade Federal do Rio Grande do Norte. Profissional de Compliance, com sete certificações nacionais e internacionais: i) Certificação Internacional em Compliance e Prevenção à Lavagem de Dinheiro (Barclays Bank); ii) Certificação em Compliance Anticorrupção CPC-A (LCB e FGV); iii) Formação executiva e certificação em Compliance na Administração Pública (Cedin); iv) Formação executiva em Compliance e Governança na Administração Pública (Insper); v) Certificação em Auditor Líder e Implementador de Sistemas de Gestão Antissuborno e Compliance ISO 37001 e ISO 19600 (Tradius); vi) Atualização da certificação Auditor Líder e Implementador de Sistemas de Gestão Antissuborno e Compliance ISO 37001 e ISO 19600 (Tradius); vii) certificação em Compliance na Saúde (Hospital Israelita Albert Einstein). Fundadora da Comissão de Compliance da OAB/RN e da ABA/RN. Possui graduação e mestrado em Ciências Jurídico-Empresariais pela Universidade Portucalense Infante D. Henrique (2010), títulos revalidados, no Brasil, pela Universidade Federal do Rio Grande do Norte (UFRN). Frequentou o Doutoramento em Ciências Jurídico-Criminais na Faculdade de Direito da Universidade de Coimbra. Avaliadora do INEP/MEC para o Ensino Superior. Investigadora do Instituto

Jurídico da Portucalense. Membro da Rede Governança Brasil (RGB). Foi Professora de Graduação em Ciências Contábeis, Administração e Direito da Universidade Federal do Rio Grande do Norte (UFRN) e Professora da Escola do Direito na Universidade Potiguar (UnP). Professora convidada de Pós-Graduação do Centro Universitário do Rio Grande do Norte (UniRN), da Universidade Potiguar (UnP) e do Centro Universitário Facex (UniFacex). Autora dos livros "Lavagem de Dinheiro e Crime Organizado" (2016), "Introdução ao Compliance (livro digital)" (2020), "Legislação Aplicada ao Compliance (livro digital)" (2020), "7 Passos para Implementar um Programa de Compliance (livro digital)" (2020) e "Compliance Bancário (livro digital)" (2020). Tem experiência na área de Compliance, Direito do Consumidor, Direito Bancário, Direito Empresarial, Direito Administrativo e Direito Penal. Atleta amadora de Jiu-Jitsu (Fx. Marron).

Calígena Batista de Paiva Silva | E-mail: caligenabpaiva@gmail.com
Aluna-pesquisadora no Grupo de Pesquisa em Compliance e Governança do Educompliance. Licenciada em Matemática (2018) pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - IFRN campus Santa Cruz. Pós-graduada em Ens. de Ciências Naturais e Matemática (2020), pelo IFRN campus Parnamirim. Atualmente cursando Bacharelado em Direito na Universidade Federal do Rio Grande do Norte - UFRN.