FUNDAÇÃO GETULIO VARGAS
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

MESTRADO PROFISSIONAL EM GESTÃO E POLÍTICAS PÚBLICAS - MPGPP

ALEXANDRE DA SILVA SANTOS

A IMPORTANCIA DA ATUAÇÃO DA AUDITORIA INTERNA NA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS EMPRESAS PÚBLICAS

SÃO PAULO
2019

ALEXANDRE DA SILVA SANTOS

A IMPORTANCIA DA ATUAÇÃO DA AUDITORIA INTERNA NA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS EMPRESAS PÚBLICAS

Artigo Individual apresentado à Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas, como requisito para a obtenção do título de Mestre em Gestão e Políticas Públicas.
Linha de pesquisa Administração Pública.
Orientador: Prof. Dr. Marco Antonio Carvalho Teixeira

SÃO PAULO
2019

RESUMO

O presente artigo tem por objetivo apontar o contexto que possibilitou a edição da Lei Geral de Proteção de Dados -13.709 - (LGPD) bem como, o impacto que o novo diploma legal causará nas empresas públicas brasileiras, que por ostentarem natureza jurídica de direito privado, independentemente do tamanho ou da complexidade da atividade explorada, deverão atender as disposições contidas na Lei 13.709.

Ressaltamos o protagonismo que o departamento de auditoria interna deverá exercer na implementação e avaliação do programa de proteção de dados pessoais, para tanto, propomos uma metodologia para elaboração de programa de auditoria, embasada numa visão holística e sistemática, orientada à avaliação de *compliance* e da eficiência e eficácia dos processos de gerenciamento de riscos, controles e governança.

Palavras-chave: Programa de Proteção de Dados; Lei Geral de Proteção de Dados; LGPD; Auditoria Interna; Empresas Públicas.

ABSTRACT

This article aims to point out the context that made it possible to issue the General Data Protection Law -13.709 - (LGPD) as well as the impact that the new legal diploma will have on Brazilian public companies, which, as they have a legal nature of private law , regardless of the size or complexity of the activity explored, must comply with the provisions contained in Law 13.709.

We emphasize the role played by the internal audit department in performing and evaluating the personal data protection program. We propose a methodology for the processing of the audit program, based on a holistic and systematic view, oriented to the evaluation of compliance and the efficiency and effectiveness of risk management, control and governance processes.

Keywords: Personal Data Protection Program; General Data Protection Law; Internal Audit Department; Public Companies.

SUMÁRIO

Introdução

A era atual pode ser considerada como a da informação, a pessoa ou empresa que domina a técnica de obtenção, análise e emprego de tal ativo mantém vantagem competitiva sobre a concorrência, a matéria prima deste bem tão precioso são os dados. Segundo David R. Anderson (et al.) (2019, p.5), "dados são os fatos e números coletados, analisados e sistematizados para apresentação e interpretação"[1].

Apesar do valor que os dados possuem para as empresas públicas, os titulares destes dados geralmente não recebem qualquer remuneração por eles, muito pelo contrário, por vezes são extraídos sem qualquer consentimento.

Os dados pessoais, por se vincularem a intimidade e a privacidade são constitucionalmente tutelados, nos termos do art. 5º inciso X da CF/88, que assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. São considerados direitos da personalidade, pois inerentes à própria condição humana.

A legislação infraconstitucional também se ocupou de proteger os dados pessoais. O Código Civil reservou um capítulo exclusivo (capítulo II) para os direitos da personalidade. Os direitos da personalidade são intransmissíveis e irrenunciáveis e o uso comercial sem autorização é vedado, conforme se depreende dos artigos abaixo colacionados.

> Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.
>
> Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.
>
> Art. 16. Toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome.
>
> Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.
>
> Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial.
>
> Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome.
>
> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

[1] ADENRSON, David R. (et al.) *Estatística aplicada a administração e economia*. Tradução da 8ª ed norte-americana 4ª ed. brasileira São Paulo: Cengage., 2019, p.5.

Além disso, no Código de Defesa do Consumidor (CDC), consta seção exclusiva (seção VI) para tratar dos direitos relacionados aos bancos de dados e cadastros de consumidores.

Na Lei consumerista são protegidos os direitos de: i) acesso às informações arquivadas, assim como das suas fontes; ii) objetividade, clareza e veracidade das informações; iii) ciência do cadastro; iv) correção dos dados inexatos e v) disponibilização em formato simples e acessível.

Inobstante todo arcabouço jurídico para proteção dos dados pessoais, a utilização sem a autorização do titular é praticada a todo momento.

Neste contexto, em 14 de agosto de 2018 foi publicada a Lei Geral de Proteção de Dados -13.709 - (LGPD), com objetivo de proteger os direitos fundamentais de liberdade, da privacidade e o livre desenvolvimento da pessoa natural, a partir da regulamentação do tratamento de dados pessoais.

De acordo com Peck (2018, p.6) a motivação para edição da Lei está relacionada ao próprio desenvolvimento do modelo de negócios da economia digital, que se consolidou a partir dos anos 1990, no qual há grande dependência dos fluxos internacionais de bases de dados, sobretudo dos dados pessoais. Acrescenta que se fez necessário "resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1944"[2].

Em razão da abrangência, complexidade e impacto da norma, a vigência ficou postergada para agosto de 2020. O prolongado *vacatio legis* se justifica pelas inúmeras adaptações que praticamente todas as empresas terão que se submeter, incluindo as empresas estatais.

Da aplicação da lei geral de proteção de dados às empresas públicas

As empresas públicas, apesar de contarem com capital integralmente público, são consideradas pessoas jurídicas de direito privado, portanto, submetem-se ao mesmo regramento da LGPD conferido às empresas privadas.

Conforme aponta Di Pietro (2014, p.521):

> Quanto à natureza jurídica das empresas públicas e das sociedades de economia mistas, as controvérsias doutrinárias se pacificaram consideravelmente a partir de 1967, de um lado, porque a Constituição, no artigo 163, §2º, determinava a

[2] PECK, Patrícia Pinheiro. *Proteção de dados pessoais: comentários à Lei nº 13.709/2018.* 1ª ed. São Paulo: Saraiva., 2018, p.6.

> submissão ao direito privado; de outro lado, tendo em vista o conceito contido no artigo 5º, II e III, do Decreto-lei nº 200.
>
> A isso tudo acrescente-se outra razão de ordem técnico-funcional, ligada à própria origem desse tipo de entidade; ela foi idealizada, dentre outras razões, principalmente por fornecer ao Poder Público instrumento adequado para o desempenho de atividades de natureza comercial e industrial; foi precisamente a forma de funcionamento e organização das empresas privadas que atraiu o Poder Público. Daí a sua personalidade jurídica de direito privado[3].

O artigo 5º, inciso II do Decreto-lei 200/67 é expresso ao atribuir personalidade jurídica de direito privado às empresas públicas.

Inobstante a natureza jurídica de direito privado, conforme sustenta Di Pietro (2014) o regime jurídico é híbrido, havendo uma derrogação parcial do direito comum pelo direito público, ou seja, o direito aplicado à empresa pública será sempre o de direito privado, quando não houver norma expressa de direito público.

Portanto, as empresas públicas deverão adequar o processo de governança para contemplar programa de proteção de dados pessoais.

Atuação da auditoria interna no programa de proteção de dados pessoais

Estar em *compliance* com a LGP não será tarefa simples e o descumprimento da lei poderá acarretar diversas sanções, inclusive multa de até 2% do faturamento da empresa, limitada a R$50.000.000,00 (cinquenta milhões), para cada infração. Tão ou mais severo que a sanção pecuniária poderá ser o dano reputacional, uma vez que a Lei prevê a possibilidade de publicização da infração. Logo, a aderência à LGPD por parte das empresas é questão cogente.

Portanto as empresas não deverão poupar esforços na implementação do programa de proteção de dados pessoais, buscando ao mesmo tempo, aderência á LGPD e aos processos de gestão de riscos e governança já existentes.

Consoante assevera Peck (2018, p.18):

> (...) dependendo do ramo do negócio, da empresa e da maturidade da governança dos dados pessoais, é fundamental criar um programa de *compliance* digital, com *risk assessment* e comunicação, *due diligence* de terceiros em um contexto multisetorial dentro do negócio e com visão holística para a legislação nacional e internacional(...)[4].

Em razão da expertise do departamento de auditoria interna, tanto na avaliação de *compliance* legal quanto da eficácia e eficiência dos processos de gerenciamento de riscos, controles internos e governança, bem como do grau de independência que referida unidade

[3] DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 27ª ed. São Paulo: Atlas, 2014.

[4] PECK, Patrícia Pinheiro. Op cit. P18.

detém, é fundamental que assuma um papel de protagonismo na implementação do programa de proteção de dados pessoais.

Na obra denominada Auditoria, de Boynton, Johnson e Kell (2002, p.31) é reproduzida definição da atividade de auditoria elaborado pelo *Report of the Committee on Basic Auditing Concepts of the American Accounting Association*: "processo sistemático de obtenção e avaliação objetivas de evidências sobre afirmações a respeito de ações e eventos econômicos, para aquilatação do grau de correspondência entre as afirmações e critérios estabelecidos, e de comunicação dos resultados a usuários interessados"[5].

Boynton, Johnson e Kell (2002, p.32) apontam que o conceito acima apresentado aborda três tipos diferentes de auditoria: auditoria de demonstrações contábeis, auditoria de *compliance* e auditoria operacional[6].

Ressaltam os autores que a auditoria de demonstrações contábeis está relacionada a obtenção e avaliação das demonstrações contábeis de uma instituição, para concluir se está aderente com os princípios contábeis geralmente aceitos.

Com relação a auditoria de *compliance*, aduzem que o objetivo é obter e avaliar evidências para determinar se as atividades desempenhadas pela organização estão aderentes à lei, aos procedimentos ou às políticas relacionados. Acrescentam também que a auditoria operacional busca avaliar a eficácia e a eficiência das atividades operacionais.

O quadro abaixo explica a diferença quanto a natureza, critérios e resultados de cada um dos mencionados tipos de auditoria.

Tipo de auditoria	**Natureza das afirmações**	**Critérios estabelecidos**	**Natureza do parecer do auditor**
De demonstrações contábeis	Dados das demonstrações contábeis	Princípios contábeis geralmente aceitos	Opinião a respeito da adequação das demonstrações contábeis
De *Compliance*	Direitos ou dados relacionados com obediência a	Políticas da administração, leis, regulamentos ou outras exigências por terceiros	Resumo dos resultados ou segurança a respeito do grau de obediência

[5] BOYNTON, Willian C, Michael B; JOHNSON, Raymond N and KELL, Walter G. *Auditoria*. São Paulo: Atlas., 2002, p.31.
[6] BOYNTON, Willian C, Michael B; JOHNSON, Raymond N and KELL. Op. cit. p. 32

	políticas, leis, regulamentos etc.		
Operacional	Dados operacionais ou de desempenho	Objetivos estabelecidos pela administração ou pela legislação	Eficiência e eficácia observadas; recomendações para aperfeiçoamento.

Fonte adaptado Boyton (2002, p.32)

De acordo com o Instituto dos Auditores Internos do Brasil (IIA Brasil):

> Auditoria interna é uma atividade independente e objetiva de avaliação e consultoria, criada para agregar valor e melhorar as operações de uma organização. Ela auxilia a organização a atingir seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada à avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, controle e governança. Sua missão é: aumentar e proteger o valor organizacional, fornecendo avaliação, assessoria e conhecimento objetivos baseados em riscos[7].

Portanto, a atuação da auditoria interna no programa de proteção de dados poderá ocorrer de duas formas distintas: a primeira, prestando consultoria para equipe multidisciplinar responsável pela implementação do programa, aproveitando assim o conhecimento holístico que a unidade possui da empresa, sobretudo quanto o grau de maturidade dos processos de gerenciamento de riscos, de controles internos e da governança. A segunda, a *posteriori*, na avaliação do programa já instalado, levantando evidências para constatar a aderência dos procedimentos à Lei 13.709/18, bem como da eficiência e da eficácia dos novos processos incorporados, emitindo as pertinentes recomendações para adequação e/ou melhoria.

Partindo-se desta premissa, o presente artigo tem por objetivo elencar os principais pontos que deverão constar num programa de auditoria para avaliação de programa de proteção de dados pessoais. Porém, faz-se necessário breves comentários sobre a LGPD.

Aspectos gerais da LGPD

A Lei nº 13.709, que entrará em vigor em agosto de 2020, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), teve inspiração no Regulamento Geral de Proteção de Dados europeu (*General Data Protection Regulation* – GDPR) em vigor desde maio de 2018.

[7] Instituto dos Auditores Internos - IIA Brasil. Disponível <www.iiabrasil.org.br>. Acesso em: 30 nov. 2019

Percebe-se, no extenso e detalhado regramento da LGPD, verdadeiro sistema de proteção de dados pessoais, onde são reforçados uma série de direitos já existentes e a criação de outros tantos para os titulares dos dados.

Para efetivar a tutela desses direitos, a LGPD impõe uma série de obrigações às pessoas jurídicas, sejam elas de natureza públicas ou privadas, inclusive às pessoas físicas, quando realizarem tratamento de dado pessoal.

Oportuno esclarecer que Tratamento de Dados consiste em toda e qualquer operação realizada com o dado pessoal, desde a coleta até o descarte. A própria LGPD exemplifica como tratamento as seguintes situações: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, comunicação, transferência, difusão ou extração.

As normas gerais contidas na LGPD são de interesse nacional e também devem ser observadas pela União, Estados, Distrito Federal e Municípios.

A LGPD terá incidência quando ocorrer alguma das seguintes situações: i) operação de tratamento realizada no território nacional; ii) atividade de tratamento cujo objetivo seja a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou iii) quando os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

Vale, ainda, destacar que, consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta, independentemente da nacionalidade do titular.

Por outro lado, a LGPD não será aplicável quando: i) o tratamento do dado for realizado em outro país sem participação de agentes de tratamento brasileiros e que não tenha sido objeto de transferência ou compartilhamento para países que não proporcionem proteção no grau compatível com a LGPD; ii) o tratamento for realizado por pessoa natural para fins exclusivamente particulares e não econômicos; iii) com fins exclusivamente jornalísticos e artísticos; iv) fins acadêmicos; v) fins de segurança pública; vi) defesa nacional, vii) segurança do Estado ou viii) atividades de investigação ou repressão a infrações penais.

Dado pessoal

Para aplicação da LGPD fundamental se faz a compreensão do que a lei define como sendo dado pessoal.

Dado pessoal é toda e qualquer informação capaz de identificar, ou tornar identificável, uma pessoa natural, de maneira direta, por exemplo: nome, registros (RG, CPF) e indireta, tais como: hábito de consumo, números de telefones, endereços, perfil, informações sobre navegação na internet (endereço de IP), etc. O critério para ser considerado dado pessoal é, portanto, a possibilidade que informação traz de identificar o titular.

Dado sensível é o dado pessoal que, além de identificar o sujeito, indica atributos relacionados à raça, credo, opinião política, filiação partidária, filiação a sindicato, opção sexual, situação de saúde, dentre outros.

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

Em contrapartida, o dado anonimizado, aquele que não permite a identificação do titular utilizando os meios técnicos disponíveis na ocasião, não goza da proteção legal. Portanto, esses dados não serão considerados dados pessoais.

Entretanto, não é qualificado como anonimizado se possível reverter o processo de anonimização, utilizando exclusivamente meios próprios ou com esforços razoáveis.

A própria LGPD define que esforço razoável deve levar em consideração fatores objetivos, a exemplo de custo e tempo necessários para reverter o processo de anonimização.

Sujeitos que atuam no sistema de proteção de dados

Ao analisarmos o ambiente de proteção de dados, instituído pela LGPD, podemos identificar os seguintes sujeitos de direito e obrigação: i) titular: pessoa natural a quem se vinculam os dados objeto de tratamento; ii) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; iii) operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria; iv) encarregado ou *Data Protection Officer* (DPO): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); v) Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A autoridade nacional poderá dispor sobre padrões de interoperabilidade, para fins de portabilidade, livre acesso aos dados, segurança bem como sobre o tempo de guarda dos

registros. A ANPD foi instituída pela Lei 13.853 de 08 de julho de 2019, com competência educadora, fiscalizatória e punitiva.

Do consentimento

Para que a empresa inicie o tratamento dos dados pessoais é imprescindível a obtenção do consentimento junto ao titular.

O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre de forma inequívoca a manifestação de vontade do titular e a finalidade do tratamento. Poderá constar diretamente em instrumento contratual, contudo, é necessário que esteja em cláusula destacada das demais.

Poderá, o consentimento, ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Vale lembrar que se trata de direito irrenunciável. Caso o tratamento envolver dados considerados sensíveis, será necessário consentimento destacado e específico. Ou seja, o cuidado deve ser intensificado nesses casos.

Se envolver dados pessoais de crianças e/ou adolescentes também se faz necessário consentimento específico e em destaque, e neste caso será concedido por um dos pais ou pelo responsável legal.

O processo para obtenção do consentimento deve ser considerado crítico ou prioritário, pois, numa eventual contenda, caberá ao controlador o ônus da prova de que foi obtido nos termos da Lei.

Em algumas situações específicas, o tratamento do dado pessoal poderá ocorrer sem o consentimento do titular, dentre as quais: i) para o cumprimento de obrigação legal ou regulatória pelo controlador; ii) para execução de contratos ou de procedimentos preliminares; iii) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; iv) para atender aos interesses legítimos da empresa responsável pelo tratamento ou aos interesses legítimos de terceiros; v) para a proteção do crédito e vi) para proteção da vida ou saúde do titular dos dados ou de terceiros.

Princípios que deverão nortear o tratamento de dados pessoais

Consoante já exposto, dentre os objetivos da LGPD destacam-se a proteção dos direitos fundamentais relacionados: a liberdade, a privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem.

Para tanto, os processos relacionados aos tratamentos de dados pessoais deverão observar, além da boa-fé, os seguintes princípios: da finalidade; da adequação; da necessidade; do livre acesso; da qualidade dos dados; da transparência; da segurança; da prevenção; da não discriminação; da responsabilização e da transparência.

Princípios da finalidade, adequação e necessidade

Os princípios da finalidade, da adequação e da necessidade são complementares, portanto devem ser analisados conjuntamente.

O princípio da finalidade estabelece que a realização do tratamento deverá atender a propósitos legítimos, específicos, explícitos e informados ao titular. Em outras palavras o tratamento se vincula aos termos do consentimento.

O princípio da adequação é decorrente do princípio da finalidade, uma vez que condiciona a compatibilidade do tratamento com as finalidades informadas ao titular.

O princípio da necessidade complementa os dois anteriores e impõe limites ao tratamento, determina que se deve ater ao mínimo necessário para a realização de suas finalidades.

Princípios da qualidade, do livre acesso e da transparência.

O princípio do livre acesso assegura aos titulares, a consulta facilitada e gratuita quanto à forma e a duração do tratamento e a integralidade de seus dados pessoais.

O princípio da qualidade dos dados determina que no tratamento deverão, ser preservados a exatidão, clareza, relevância e atualização dos dados.

O princípio da transparência reforça os anteriores e ratifica que as informações devem ser claras, precisas e facilmente acessíveis, inclusive quanto os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Princípios da prevenção e segurança

Os princípios em epigrafe estabelecem que deverão ser empregadas todas as medidas, técnicas e administrativas, aptas a proteger os dados pessoais, evitando a ocorrência de danos em virtude do tratamento de dados pessoais.

Princípio da não discriminação

O princípio da não discriminação proíbe o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

Direitos do titular

Como o próprio nome sugere, os dados pessoais são de titularidade da pessoa aos quais se referem, na relação jurídica de tratamento de dados surgem uma série de direitos ao titular, que poderá exercê-los a qualquer momento, dentre os quais destacamos: i) não fornecer ou revogar o consentimento; ii) confirmação do tratamento; iii) acesso aos dados; iv) correção; v) anonimização, bloqueio ou eliminação de dados desnecessários; vi) portabilidade; vii) direito de petição; viii) direito de oposição; ix) eliminação dos dados e x) revisão de decisões baseadas em tratamento automatizado de dados pessoais.

Consoante já ressaltamos, é imprescindível para que se inicie o tratamento de dados pessoais o consentimento por parte do titular, por consequência lógica, a Lei assegura a possibilidade da não autorização bem como da revogação, a qualquer momento, do consentimento. Aqui vale ressaltar que o consentimento se refere a um direito irrenunciável e intransferível, qualquer situação que afrontar esta questão será nula.

O direito de confirmação do tratamento está aderente ao princípio da transparência, referido direito resguarda ao titular a ciência de que seus dados pessoais são ou não objeto de tratamento.

Também é assegurado ao titular o acesso facilitado e gratuito às informações sobre o tratamento de seus dados, para esclarecimentos quanto à finalidade, forma e duração do tratamento, identificação e contato do controlador, eventual uso compartilhado e finalidade do compartilhamento. Em aderência aos princípios do livre acesso e da transparência.

O direito de correção de dados incompletos, inexatos ou desatualizados é uma decorrência dos princípios da qualidade, da exatidão, clareza, relevância e atualização dos dados. Ao titular é garantido que os dados pessoais considerados desnecessários sejam anonimizados, bloqueados ou até mesmo eliminados, em consonância com o princípio da necessidade.

Além disso, é resguardado ao titular a portabilidade dos dados pessoais a outro fornecedor, portanto, em contrapartida é obrigação do agente de tratamento fornecer os dados tratados em formato corriqueiramente usado, permitindo, assim, o êxito da portabilidade.

Outro direito conferido ao titular dos dados pessoais é o de peticionar em relação aos seus dados em face do controlador junto à autoridade nacional de dados, ou seja, poderá formular reclamações perante a ANPD.

De acordo com o direito de oposição, o titular poderá obstar o tratamento de dados realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento aos dispositivos da LGPD.

Por fim, destacamos o direito do titular de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado, exemplo de tratamentos automatizados: para definir o perfil de consumo e de crédito.

Término do tratamento e eliminação dos dados

O tratamento do dado pessoal deve ser compreendido como um processo, e como tal, tem início, meio e fim.

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: i) finalidade alcançada; ii) fim do período de tratamento; iii) revogação do consentimento; iv) por determinação da ANPD ou v) quando houver violação às disposições da LGPD.

Verificado o término do tratamento, os dados pessoais deverão ser eliminados. A manutenção será permitida para cumprimento de obrigação legal ou se os dados forem anonimizados. Os princípios da prevenção e da segurança também deverão ser observados na eliminação dos dados.

Governança e boas práticas

Não basta a constituição de um ambiente seguro sob a ótica de proteção de dados, a empresa também deve demostrar tais ações à sociedade (*accountability).*

Neste sentido, o controlador e operador deverão implementar medidas de segurança, capazes de proteger os dados pessoais contra acessos não autorizados e situações acidentais que ocasione destruição, alteração ou comunicação dos dados pessoais.

É importante que os agentes de tratamento estabeleçam regras de boas práticas e de governança para mitigar os riscos apontados na LGPD, inclusive com a elaboração de procedimentos que assegurem os direitos do titilar.

A LGPD elenca uma série de procedimentos mínimos que deverão constar nos programas de governança de proteção de dados pessoais:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação;
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

A adoção de boas práticas, além de mitigar riscos e por consequência minimizar danos, também poderá servir como atenuante em eventuais sanções recebidas.

Do Relatório de impacto à proteção de dados pessoais

O relatório de impacto à proteção de dados pessoais é documento de responsabilidade do controlador no qual deverão ser registrados todos os processos relacionados ao tratamento de dados pessoais.

Neste documento também deverão conter, detalhadamente, todas as medidas implementadas para gerenciamento e mitigação dos riscos bem como as ações para resguardar os princípios e direitos do titular dos dados, previstos na LGPD.

Feitas essas considerações podemos avançar para análise dos pontos que o programa de auditoria deverá abordar.

Programa de auditoria interna relacionado à LGPD

Programa de auditoria, conforme Boynton (2002, p.220): “registra os procedimentos que o auditor acredita serem necessários à consecução dos objetivos da auditoria. A forma do programa varia com as circunstâncias e com as práticas e políticas da empresa de auditoria. O programa também documenta a estratégia da auditoria que será seguida (...)”

Nesta linha de raciocínio, o programa de auditoria interna relacionado à LGPD deverá ser abrangente e contemplar os principais aspectos disciplinados na Lei 13.709/18.

Para tanto, propomos que seja divido em oito grupos de testes, para avaliação dos seguintes pontos: i) forma de tratamento e consentimento; ii) observância aos direitos fundamentais; iii) observância dos princípios; iv) requisitos técnicos de TI; v) existência de processos obrigatórios e atenção aos direitos do titular; vi) governança; vii) relatório de impacto de dados e viii) avaliação das atividades do Encarregado pelo tratamento de dados pessoais (DPO).

No grupo de testes 1 "Tratamento dos dados e Consentimento", o objetivo será avaliar a forma de tratamento dos dados pessoais e se o consentimento atende aos requisitos legais. Para tanto, sugerimos que sejam percorridos os seguintes quesitos:

- qual(is) especie(s) de tratamento de dados a empresa executa?
- qual é a hipótese para legitimar o tratamento?
- se a hipótese para legitimar o tratamento for o consentimento:
- o titular consentiu de forma livre?
- o consentimento é demonstrado de forma inequívoca?
- o titular foi orientado de forma clara e inequívoca antes de consentir?
- o consentimento refere-se a uma finalidade determinada?
- há tratamento de dados sensíveis?
- há consentimento específico quanto ao tratamento dos dados sensíveis?
- há tratamento de dados de criança ou adolescente?
- há consentimento dos pais ou responsável legal?
- há compartilhamento de dados?
- o compartilhado mantém programa de proteção de dados pessoais?

No grupo de testes 2 "Direitos Fundamentais", o objetivo será avaliar se o processo de tratamento de dados pessoais preserva os direitos fundamentais. Desta forma, os seguintes pontos deverão ser abordados.

- está preservado o respeito à privacidade?
- está preservada a autodeterminação informativa?
- estão preservadas a liberdade de expressão, de informação, de comunicação e de opinião?
- estão preservadas a inviolabilidade da intimidade, da honra e da imagem?

- estão preservados o desenvolvimento econômico e tecnológico e a inovação?
- estão preservadas a livre iniciativa, a livre concorrência e a defesa do consumidor?
- estão preservados os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais?
- está preservada a não discriminação?

O Grupo de testes 3 "Princípios" terá como objetivo analisar se os princípios expressos na LGPD foram observados no processo. Assim, propomos os seguintes questionamentos para serem respondidos.

- é observado o princípio da finalidade?
- é observado o princípio da adequação?
- é observado o princípio da necessidade?
- há processo que permite o livre acesso ao titular sobre o processo de tratamento?
- há controle quanto a qualidade dos dados?
- é observado o princípio da transparência?

O grupo de testes 4 "Questões Técnicas de TI" deverá ser executado por auditores especialistas em TI, com o objetivo de evidenciar se são adotadas medidas técnicas aptas a proteger os dados pessoais de acessos não autorizados. Ao final dos testes os questionamentos abaixo deverão ser respondidos.

- são adotadas medidas técnicas aptas a proteger os dados pessoais de acessos não autorizados?
- são adotadas medidas técnicas aptas a proteger os dados pessoais de situação acidentais ou ilícitas de destruição?
- são adotadas medidas técnicas aptas a proteger os dados pessoais de situação acidentais ou ilícitas de perda?
- são adotadas medidas técnicas aptas a proteger os dados pessoais de situação acidentais ou ilícitas de alteração?
- são adotadas medidas técnicas aptas a proteger os dados pessoais de situação acidentais ou ilícitas de comunicação?
- são adotadas medidas técnicas aptas a proteger os dados pessoais de situação acidentais ou ilícitas de difusão?

O grupo de testes 5 "Processos Obrigatórios e Direitos do Titular", analisará se os processos obrigatórios foram implementados pela empresa, assim como se há mecanismos para viabilizar os direitos dos titulares dos dados. Para tanto, os pontos abaixo deverão ser enfrentados.

- há processo para viabilizar direito do titular?
    i) processo para revogar o consentimento;
    ii) processo para confirmação do tratamento;
    iii) processo que garanta de forma gratuita e facilitada acesso aos dados;
    iv) processo que permita ao titular solicitar correção de dados incompletos, inexatos ou desatualizados;
    v) processo de anonimização, bloqueio ou eliminação de dados desnecessários;
    vi) processo para viabilizar a portabilidade;
    vii) gestão e tratamento das reclamações relacionadas a tratamento de dados pessoais;
    viii) possibilidade do titular pedir revisão de decisões com base em tratamento automatizado de dados pessoais
- há processo para comunicação de incidente de segurança?
- há processo para eliminação dos dados?

No grupo de testes 6 "Governança", será avaliado a existência, abrangência, a eficiência e eficácia dos processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais, o que poderá ser constatado percorrendo os quesitos abaixo.

- foram estabelecidas políticas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade?
- foram estabelecidos mecanismos de *accountability*?
- os mecanismos de governança relacionados a proteção de dados estão integrados à estrutura geral de governança inclusive os processos de gerenciamento de riscos e controles internos?
- há planos de resposta a incidentes e remediação devidamente registrados?

No grupo de testes 7 "Relatório de Impacto de Proteção de Dados" terá por objetivo avaliar a existência, completude e devido arquivo do relatório de impacto de proteção de dados.

Recomendamos que os testes relacionados a este grupo sejam realizados por último, entretanto, é fundamental que o auditor utilize o Relatório de Impacto de Proteção de Dados para subsidiar os demais testes. O presente teste buscará responder aos seguintes pontos:

- o relatório de impacto à proteção de dados pessoais elenca os processos de tratamento de dados pessoais, considerados críticos?
- o relatório de impacto à proteção de dados pessoais informa a relação das ações implementadas para assegurar os princípios e direitos do titular dos dados, previstos na LGPD?
- o relatório de impacto à proteção de dados pessoais registra a descrição do gerenciamento de riscos, controles, boas práticas e governança implementados?

No grupo de teste 8 "DPO", serão avaliadas as atividades desempenhadas pelo DPO, para obter evidências se estão ou não em aderência às disposições da LGPD, assim, imprescindível enfrentar os seguintes pontos.

- houve nomeação de DPO?
- há divulgação no site da empresa com relação aos dados do DPO, de forma clara objetiva e de fácil visualização?
- existe canal de comunicação para o titular formular reclamações?
- há estrutura compatível para aceitar e responder as reclamações e comunicação dos titulares?
- há estrutura compatível para aceitar e responder as reclamações e comunicação da ANPD?
- há estrutura compatível para receber e adotar as providencias da ANPD?
- há atuação eficaz e eficiente do DPO no sentido de orientar os funcionários com relação as disposições da LGPD?

Conclusão

Diante dos desafios do mundo moderno é impensável a exploração de atividade econômica sem que haja a utilização de dados pessoais, vivemos na era da informação e numa sociedade digital.

Esse ambiente, entretanto, não pode servir como salvo-conduto para revogação tácita de direitos constitucionalmente assegurados, muito pelo contrário, este cenário deve impulsionar

o fortalecimento do arranjo institucional que preserve o cidadão, pois quanto maior o avanço tecnológico maior é a possibilidade de obtenção e utilização indevida dos dados pessoais.

Assim, plenamente justificada a elaboração da LGPD com previsão de inúmeras obrigações e severas penalizações.

A correta implementação da LGPD nas empresas públicas não será tarefa fácil, fundamental a elaboração de um programa de proteção de dados pessoais que percorra todo o ambiente corporativo, inclusive com alcance dos parceiros comercias.

A auditoria interna, por atuar com independência e pela expertise na avaliação de *compliance* legal e da eficácia e eficiência dos processos de gerenciamento de riscos, controles internos e governança, terá um papel de protagonismo no programa de proteção de dados pessoais.

Desta forma, é imprescindível que a auditoria interna estabeleça um programa de auditoria orientado por uma visão holística, capaz de avaliar a efetividade do programa de proteção de dados em sua integralidade, promovendo a melhoria continua da governança de dados, contribuindo, assim, não somente para sustentabilidade da empresa, mas também para o desenvolvimento humano da sociedade digital.

REFERÊNCIAS

ADENRSON, David R. (et al.) **Estatística aplicada a administração e economia**. Tradução da 8ª ed norte-americana 4ª ed. brasileira São Paulo: Cengage, 2019.

ATTIE, Willian. **Auditoria**. São Paulo: Atlas., 1998.

BOYNTON, Willian C, Michael B; JOHNSON, Raymond N and KELL, Walter G. **Auditoria**. São Paulo: Atlas., 2002.

BRASIL. **Constituição da República de 1988**. Disponível <http://www.planalto.gov.br> . Acesso em 20 nov. 2019.

BRASIL. Lei 8.078 de 11 de setembro de 1990, **Código de Defesa do Consumidor**. Disponível <http://www.planalto.gov.br>.Acesso em 20 nov. 2019.

BRASIL. lei 10.406 de 10 de janeiro de 2002, **Código Civil**. Disponível <http://www.planalto.gov.br>. Acesso em 20 nov. 2019.

BRASIL. Decreto-lei 200 de 25 de fevereiro de 1967. Disponível <http://www.planalto.gov.br>. Acesso em 20 nov. 2019.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Disponível <http://www.planalto.gov.br>. Acesso em 20 nov. 2019.

BRASIL. Lei 13.853 de 08 de julho de 2019. Disponível <http://www.planalto.gov.br>. Acesso em 20 nov. 2019.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 27ª ed. São Paulo: Atlas, 2014.

INSTITUTO DOS AUDITORES INTERNOS - IIA Brasil. Disponível <www.iiabrasil.org.br>. Acesso em: 30 nov. 2019.

PECK, Patrícia Pinheiro. *Proteção de dados pessoais: comentários à Lei nº 13.709/2018.* 1ª ed. São Paulo: Saraiva., 2018.