UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

MATHEUS BRAGA BENEDITO

LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE SOBRE OS DIREITOS DOS TITULARES E OS DEVERES DAS ORGANIZAÇÕES PERANTE A LEI

CAMPINA GRANDE - PB

2021

MATHEUS BRAGA BENEDITO

LEI GERAL DE PROTEÇÃO DE DADOS: UMA ANÁLISE SOBRE OS DIREITOS DOS TITULARES E OS DEVERES DAS ORGANIZAÇÕES PERANTE A LEI

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Orientador: Pedro Sergio Nicolletti

CAMPINA GRANDE - PB

2021

B4631 Benedito, Matheus Braga.

Lei geral de proteção de dados: uma análise sobre os direitos dos titulares e os deveres das organizações perante a lei. / Matheus Braga Benedito. – 2021.

14 f.

Orientador: Prof. Me. Pedro Sergio Nicolletti.

Trabalho de Conclusão de Curso - Artigo (Curso de Bacharelado em Ciência da Computação) - Universidade Federal de Campina Grande; Centro de Engenharia Elétrica e Informática.

1. Lei geral de proteção de dados. 2. Dados – proteção. 3. Privacidade de dados. 4. Dados pessoais – proteção. 5. Tratamento de dados. 6. Dado anonimizado. 7. Legislação sobre dados. 8. Ciclo de vida dos dados. 9. Criptografia da informação. 10. Política de segurança da informação. 11. Segurança da informação. I. Nicolletti, Pedro Sergio. II. Título.

CDU:004.6:34(045)

Elaboração da Ficha Catalográfica:

Johnny Rodrigues Barbosa
Bibliotecário-Documentalista
CRB-15/626

MATHEUS BRAGA BENEDITO

LEI GERAL DE PROTEÇÃO DE DADOS:

UMA ANÁLISE SOBRE OS DIREITOS DOS TITULARES E OS DEVERES DAS ORGANIZAÇÕES PERANTE A LEI

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA:

Professor Pedro Sergio Nicolletti

Orientador – UASC/CEEI/UFCG

Professor Reinaldo Cézar de Morais Gomes

Examinador – UASC/CEEI/UFCG

Professor Tiago Lima Massoni

Professor da Disciplina TCC – UASC/CEEI/UFCG

Trabalho aprovado em: 25 de maio de 2021.

CAMPINA GRANDE - PB

ABSTRACT

In order to create a legal protection regarding the privacy and protection of users' digital personal data on the internet, the General Data Protection Law was created, which regulates all data processing of Brazilian citizens inside and outside Brazil. This work proposes to present an analysis on the main points of the normative set of the law, in an approach focused on the rights of the owners, security and governance practices that developers and companies must adopt to guarantee compliance with the law's proposals, through a broad research using in addition to the full text of the law, scientific articles in correlated areas and information available on government websites, with the aim of linking what was proposed in law with the practice from the point of view of the user and organizations.

Key words: General Data Protection Law, holders' rights, compliance, governance.

Lei Geral de Proteção de Dados:

Uma análise sobre os direitos dos titulares e os deveres das organizações perante a lei.

Matheus Braga Benedito
matheus.benedito@ccc.ufcg.edu.br
Unidade Acadêmica de Sistemas e Computação
Universidade Federal de Campina Grande, Paraíba

Pedro Sergio Nicolletti
peter@computacao.ufcg.edu.br
Unidade Acadêmica de Sistemas e Computação
Universidade Federal de Campina Grande, Paraíba

RESUMO

Com o intuito de criar um amparo legal quanto à privacidade e à proteção de dados pessoais digitais de usuários na internet, foi criada a Lei Geral de Proteção de Dados, que regula todo tratamento de dados de cidadãos brasileiros dentro e fora do Brasil. Este trabalho se propõe a apresentar uma análise sobre os principais pontos do conjunto normativo da lei, numa abordagem voltada aos direitos dos titulares, práticas de segurança e governança que desenvolvedores e empresas devem adotar para garantir conformidade com as propostas da lei, por meio de uma pesquisa ampla utilizando além do texto integral da lei, artigos científicos em áreas correlacionadas e informações dispostas em sites governamentais, com o objetivo de relacionar o que foi proposto em lei com a prática do ponto de vista do usuário e organizações.

Palavras-chave

LGPD, direitos dos titulares, conformidade, governança.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), aprovada em agosto de 2018 e com vigência a partir de setembro de 2020, propõe uma padronização de normas e práticas, para assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, de forma igualitária dentro do país e no mundo, não importando se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de conteúdo de pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser cumprida.

A lei estabelece o que são dados pessoais, quais dados estão sujeitos a cuidados ainda mais específicos, como o caso de dados sensíveis e os sobre crianças e adolescentes, estabelece também a maneira como empresas e órgãos públicos tratam a privacidade e a segurança das informações de usuários e clientes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação.

Este trabalho se propõe a apresentar uma análise sobre os principais pontos do conjunto normativo da lei, esclarecendo os direitos dos usuários e sugerindo práticas de segurança e governança a serem adotadas por organizações para garantir conformidade com as propostas da lei, utilizando além do texto integral da lei, artigos científicos em áreas correlacionadas e informações dispostas em sites governamentais, com o objetivo de relacionar o que foi proposto em lei com a prática do ponto de vista do usuário e organizações.

2. FUNDAMENTAÇÃO TEÓRICA

A LGPD altera alguns artigos do Marco Civil da Internet e estabelece novas regras para empresas e órgãos públicos no que diz respeito ao tratamento da privacidade e segurança das informações de usuários e clientes.

O ponto central da nova lei é que nenhuma instituição pode utilizar os dados de nenhum cidadão sem o seu consentimento explícito. O texto também traz garantias para o usuário, que pode solicitar que seus dados sejam deletados, revogar um consentimento, transferir os dados para outro fornecedor de serviços, entre outras ações. E o tratamento dos dados deve ser feito levando em conta alguns quesitos, como finalidade e necessidade, que devem ser previamente acertados e informados ao cidadão. Com a entrada em vigor da lei, as empresas terão que observar alguns procedimentos para obter dados dos clientes, bem como para arquivá-los e tratá-los, devendo alterar suas rotinas e processos.

As sanções administrativas a serem aplicadas a quem desrespeitar as regras do tratamento de dados pessoais por força da Lei 14.010/20, entram em vigor a partir de 1º de agosto de 2021, as punições podem chegar até 2% do faturamento, com um limite de até 50 milhões de reais.

3. METODOLOGIA

Para o desenvolvimento desta pesquisa, de caráter observacional, realizamos uma revisão sistemática da literatura, utilizando o texto integral da lei, guias sobre a LGPD publicados no domínio gov.br e artigos científicos selecionados por palavras-chave como: “LGPD”, “governança”, “segurança da informação”.

Após a fase de seleção, realizamos então uma análise que pudesse utilizar dos resultados e discussões do material fonte selecionado, objetivando esclarecer os principais pontos da lei, os direitos dos titulares dos dados, e os deveres que as organizações têm perante à lei, e além disso, propor uma série de sugestões para que empresas revejam seus processos, e caso necessário, os adequem para que haja conformidade com a lei, e propor também sugestões de técnicas de segurança da informação, para que se minimize os riscos existentes de acesso indevido durante o tratamento de dados pessoais e se evite a penalização por desconformidade com a LGPD.

4. DEFINIÇÕES

A LGPD em seu artigo 5º traz definições fundamentais sobre dados pessoais e entidades envolvidas no seu tratamento [1]:

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

2. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, etc;

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

Estas definições são de extrema importância, pois são elas que provêem uma base para todo o corpo da lei, diferenciando os tipos de dados tratados, podendo assim haver uma especificidade de tratamento para cada um deles, bem como podem ser usadas pela Autoridade Nacional de Proteção de Dados (ANPD) para averiguação dos tipos de dados presentes em casos de violação de privacidade, podendo assim ser tomada as devidas ações com base no tipo de dado violado.

Para identificar as atividades e os respectivos responsáveis no tratamento de dados pessoais a LGPD define quatro entidades [1]:

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

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

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

4. Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Estas entidades, são definidas pela lei para que haja um esclarecimento do papel de cada uma delas no tratamento de dados pessoais, e para que seja possível identificar em casos de descumprimento com a lei, o devido responsável para que a ANPD possa seguir com o cumprimento das sanções.

5. TRATAMENTO DE DADOS

A LGPD previu expressamente em seu artigo 7°, dez hipóteses que autorizam o tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais.

Na sequência, são apresentadas as considerações mais relevantes sobre as hipóteses legais de tratamento de dados da LGPD para o escopo deste artigo:

I - Mediante o fornecimento de consentimento pelo titular.

Hipótese que exige consentimento do titular do dado. É a manifestação livre e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, tem liberdade para autorizar, negar ou revogar (reconsiderar) autorização anteriormente concedida para tratamento de seus dados pessoais. A manifestação de vontade precisa ser (I) livre e inequívoca; (II) formada mediante o conhecimento de todas as informações necessárias para tal, o que inclui a finalidade do tratamento de dados e eventual compartilhamento; e (III) restrita às finalidades específicas e determinadas que foram informadas ao titular dos dados. O ônus da prova do consentimento cabe ao controlador.

O controlador que obtiver o consentimento e necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas em lei.

II - Para o cumprimento de obrigação legal ou regulatória pelo controlador.

Hipótese que dispensa o consentimento do titular do dado. É a regra da legalidade ampla e da preservação do interesse público sobre o particular. Esse é um autorizador da LGPD que possibilita que a lei não entre em conflito com outras legislações ou regulamentos vigentes.

IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Hipótese que dispensa o consentimento do titular do dado. É uma previsão geral e subsidiária, mediante prévia e expressa motivação pelo controlador da finalidade e necessidade (legítimo interesse) do tratamento.

O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I – apoio e promoção de atividades do controlador; II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da LGPD.

Em tais circunstâncias, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo o controlador adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Ainda sobre o tratamento de dados, é preciso esclarecer que, por taxativa previsão da LGPD (Art. 4°), as disposições da lei não são aplicadas ao tratamento de dados pessoais nas seguintes situações [1]: I - Realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - Realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os artigos. 7º e 11 da LGPD); III - realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou; IV - Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

6. DIREITOS DOS TITULARES

Existe uma lista de direitos previstos para o titular dos dados no artigo 18 da LGPD [1] que devem ser assegurados enquanto seus dados forem processados:

1. Direito de Confirmação da Existência de tratamento dos dados;

2. Direito de acesso aos dados;

3. Direito de correção de dados incompletos, inexatos ou desatualizados;

4. Direito de anonimização, bloqueio ou eliminação de dados desnecessários;

5. Direito de portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

6. Direito de eliminação dos dados tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16;

7. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

8. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

9 - Revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

Além de uma série de outros direitos específicos espalhados pelo texto da lei [1], como:

• Exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento, Art. 7º, § 6º.

• Inversão do ônus da prova quanto ao consentimento, art. 8º, § 2º.

• Requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais, art. 8º, § 4º.

• Ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento, art. 8º, § 6º.

• Anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa, art. 11 II.

• Impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular), art. 11, § 4º.

• Revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20).

Quando o titular dos dados necessitar gozar de seus direitos, deverá contatar diretamente o encarregado de dados da empresa, esta deve manter as informações sobre o encarregado de maneira pública e acessível aos consumidores, incluindo meios de contato para que os titulares possam solicitar quaisquer ações que lhe são de direito.

A petição deve ser respondida com agilidade, clareza e completude, sob pena de o titular dos dados ter a prerrogativa de representar contra o responsável na ANPD, organismos de defesa do consumidor ou ajuizar pretensão com tal causa de pedir. Na impossibilidade de atendimento imediato do requerimento do titular do dado pessoal, o controlador poderá comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência [2].

O não cumprimento de tais direitos pode ser comunicada a ANPD que passaria a analisar e intervir no caso podendo aplicar multas pelo descumprimento da lei.

7. ADEQUAÇÃO DAS EMPRESAS À LGPD

O processo de adequação à LGPD está ligado à revisão dos processos do negócio. Partindo do princípio de que um processo de negócio compreende o conjunto de um ou mais procedimentos ou atividades relacionadas, as quais, coletivamente, realizam um objetivo de negócio no contexto de uma estrutura organizacional pode-se de dizer que é o processo de negócio que determina como o trabalho será executado na organização e toda a sequência lógica das atividades. Sendo assim, se o processo aborda questões de privacidade e conformidade com a LGPD, dificilmente uma organização sofrerá com as sanções da lei [3].

Junior propôs em seu trabalho [3] um questionário de avaliação de conformidade com objetivo de responder a pergunta "Como avaliar a conformidade de um processo de negócio com a LGPD?" As perguntas que compõem o questionário foram definidas com base nos direitos do titular e nos textos da lei brasileira, de forma que existisse uma coesão entre o que o questionário almejava e o que a lei determina.

Após responder as questões presentes no questionário de avaliação, para determinar se o processo de negócio está em conformidade com a LGPD, as respostas para todas as questões devem ser “Sim” quanto à modelagem das ações necessárias ou “Não aplicável”. Portanto, como todas as ações são necessárias para atingir a conformidade, não existe um número mínimo de respostas "Sim"/"Não aplicável" para que um processo de negócio possa ser considerado compatível com a LGPD.

Apresentamos as questões que compõe o questionário bem como sua referência legislativa na LGPD:

1. O processo inclui as ações para obter consentimento? Segundo o art. 7º, faz-se necessário que o controlador obtenha o consentimento do usuário para que possa iniciar o tratamento dos dados com ressalva para quando os dados foram tornados públicos pelo usuário, como fica registrado no § 4°.

2. O processo especifica as bases legais de processamento? O controlador poderá tratar dados pessoais (art. 7 - §II a §X) ou dados sensíveis (art.11 - §II) mesmo sem ter consentimento do usuário desde que apresente base legal para o tratamento dos dados. Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados, garantindo-lhes o exercício dos direitos previstos no art. 18 da LGPD.

3. O processo inclui as ações para lidar com dados pessoais de crianças? Como citado no art.14, §I: O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Portanto, o controlador poderá tratar dados pessoais de crianças somente com consentimento específico que deve ser cedido por pelo menos um dos pais ou guardião legal do menor.

4. O processo contém informações sobre a possibilidade de não prover consentimento e as consequências da recusa? Conforme art. 18, inciso VIII, o controlador é obrigado a ceder ao titular dos dados as informações sobre a possibilidade de não fornecer o seu consentimento para tratamento de dados e bem como as consequências da negação.

5. O processo contém as ações para compartilhamento de dados com terceiros? Como estabelecido no art. 7, § 5º no caso de compartilhamento de dados com terceiros, o titular deve ficar ciente por meio do consentimento específico para este fim.

6. O processo inclui as ações para lidar com dados sensíveis? O Art. 11 diz que: O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses [1]: I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; Porém os dados sensíveis podem ser tratados em ocasiões específicas sem o consentimento de um titular, como diz a cláusula II: sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a)

cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; [1]. É essencial que as empresas se enquadrem em alguma das hipóteses de tratamento de dados pessoais sensíveis previstas no art. 11 da lei, pois este tipo de dado tratado de maneira indevida poderá ser um agravante em caso de ações tomadas pela ANPD.

7. O processo indica quem é o ator (departamento/posição) responsável pelo processamento de dados em cada atividade? Faz-se necessário saber quem é responsável pelo processamento de dados em cada etapa do processamento, para que em casos como os citados no art.42, (que atribui a responsabilidade de danos morais ou patrimoniais ocasionados no tratamento de dados pessoais ao controlador ou operador que o ocasionou, atribuindo ainda obrigação de reparo) seja identificado o ator a ser responsabilizado, ou ter isenção de responsabilidade como trata o art. 43 [1]: Os agentes de tratamento só não serão responsabilizados quando provarem: I - Que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - Que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

8. O processo apresenta a finalidade de processamento dos dados no nome do modelo? Um processo que possui sua finalidade logo no nome de seu modelo pode facilmente ser identificado pelo titular de forma clara e concisa de que seus dados estão sendo tratados para a finalidade descrita no documento de consentimento, respeitando assim o art.9 da LGPD.

9. O processo apresenta o local em que os dados são armazenados e processados? Pelo art. 19: A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso [1]. Prover o local de armazenamento e processamento de dados facilita o atendimento da solicitação de acesso de dados, visto que esse é um direito dos titulares e pode ser solicitado a qualquer momento.

10. O processo inclui as ações para realizar uma transferência internacional de dados? Existem algumas restrições quanto à possibilidade de realizar uma transferência internacional de dados, as permissões para tal estão definidas no art. 33, sendo a principal delas citada no inciso I: I - Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta lei [1]. Além de precisar de se enquadrar em uma das hipóteses previstas no art.33, é preciso que, pelo art.34 o nível de proteção de dados do país estrangeiro ou do organismo internacional para a qual será feita a transferência seja compatível com a avaliação da autoridade nacional, que levará em consideração os incisos I a VI do art.34.

11. O processo inclui as ações para descarte de dados? O art.16 trata da eliminação dos dados pessoais após o seu término de tratamento, trazendo as hipóteses de conservação de tais dados, portanto os dados pessoais devem ser descartados ao término de seu processamento a menos que se enquadre em alguma das afirmativas presentes no artigo.

12. O processo inclui as ações para realizar portabilidade de dados? A portabilidade dos dados só deve ser realizada mediante solicitação expressa do titular dos dados e apenas dados não anonimizado pelo controlador podem ser transferidos, conforme art.18, inciso V complementado pelo § 7°.

13. O processo inclui as ações para lidar com um vazamento de dados? Pelo art. 48, o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares [1]. O comunicado deve conter informações sobre os titulares que foram envolvidos no vazamento, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial, entre outras informações. A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - Ampla divulgação do fato em meios de comunicação; e II - Medidas para reverter ou mitigar os efeitos do incidente [1].

14. O processo inclui as ações para realizar decisões automatizadas? Conforme proposto no art.20, o controlador tem o dever de informar ao titular dos dados sobre as tomadas de decisão automatizadas baseadas no perfil que foi traçado para o titular dos dados.

15. O processo inclui as ações para o caso de haver revogação de consentimento? A lei trata em seu § 5° do art. 8 desse direito do titular, portanto, em caso de revogação de consentimento o tratamento de dados do titular deve ser imediatamente cessado, o que acarreta em alterações no processo para poder lidar com o término de tratamento de dados antes do prazo idealizado inicialmente.

16. O processo inclui as ações a serem tomadas no caso de haver uma solicitação de retificação de dados? O art. 18 em seu inciso III traz o direito do usuário de correção de dados incompletos, inexatos ou desatualizados, logo, o titular pode retificar os dados a qualquer momento, é necessário estar apto a atender este tipo de solicitação.

17. O processo inclui as ações a serem tomadas no caso de uma solicitação de acesso de dados por parte do usuário? Atendendo ao princípio do livre acesso o art. 9 trata do direito do usuário de acesso facilitado às informações sobre o tratamento de seus dados, portanto o processo deve prover ações para tal acesso de informações.

Responder ao questionário, significa fazer uma análise do modelo do negócio atual e identificar os pontos do processo que precisam ser ajustados para entrarem em conformidade com a LGPD.

Além de rever e ajustar os processos, as empresas precisam definir os indivíduos que atuarão como controlador, operador e encarregado de dados. A identificação dos controladores depende necessariamente, em cada situação, da existência da capacidade de decidir sobre os meios e a finalidade do tratamento de dados. Assim, serão considerados controladores, por exemplo, os órgãos públicos que contratarem empresa privada para gerir seu registro de visitantes, na medida em que tal empresa agirá sob as ordens do órgão contratante. Nessa ilustração, o órgão contratante (controlador) não apenas estabelecerá a finalidade do tratamento, mas também exigirá da empresa contratada (operador) a adoção dos meios técnicos necessários para garantir a observância dos princípios que regem o tratamento dos dados pessoais, especificados no art. 6º da LGPD. Para distinguir entre controlador e operador, portanto, é fundamental reconhecer qual ente possui autonomia decisória quanto a fins e meios de tratamento (controlador), e qual possui escopo eminentemente executório (operador), submetido aos desígnios de outrem [2].

O estabelecimento dessas entidades é fundamental para conformidade com a lei, pois além de atribuir a cada uma delas suas

respectivas responsabilidades no tratamento dos dados, este é um ponto fundamental para eventuais investigações pela ANPD, que precisa saber quem é responsável pelo processamento de dados em cada etapa do processamento para poder atribuir responsabilidade por eventuais danos causados aos titulares.

Por fim, as empresas precisam elaborar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que representa um documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados [2]. Segundo o inciso XVII do art. 5º da LGPD, o RIPD é a documentação que deve ser mantida pelo controlador dos dados pessoais.

O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados [1].

Casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado [2]:

• Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

• Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados);

• A qualquer momento sob determinação da ANPD (art. 38).

Quando for necessária a elaboração do RIPD, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.

O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição. Serve tanto para a análise quanto para a documentação. É importante que as empresas possuam um modelo genérico do RIPD para que este possa ser ajustado de acordo com eventuais solicitações da ANPD, permitindo assim que haja uma resposta à mesma em tempo hábil.

O RIPD pode servir como um documento de defesa para as empresas em casos de ações da ANPD referentes a algum descumprimento da lei, podendo este servir como um atenuante das sanções aplicadas à empresa pela ANPD, daí a importância de possuir um RIPD bem elaborado, atualizado e que contenha todas as informações de segurança adotadas pela empresa.

7.1 Comunicação de incidentes de segurança

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais [6].

O art. 48 da LGPD determina que é obrigação do controlador comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A empresa deve avaliar internamente o incidente, sua natureza, categoria e quantidade dos dados afetados, consequências concretas e prováveis. A comunicação à ANPD deve conter no mínimo os itens descritos no § 1º do artigo 48 da LGPD, sugerimos o preenchimento do formulário de comunicação de incidente de segurança à ANPD, disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, que apresenta um modelo padronizado com todos os itens obrigatórios que devem ser enviados, bem como itens adicionais que irão servir tanto para auxiliar a ANPD no momento em que o órgão processar a análise do incidente, quanto como um possível atenuador em caso da aplicação de sansões administrativas, desde que o relatório apresente um alto grau de detalhamento do incidente, incluindo todas as medidas de segurança adotadas para prevenir o incidente que ocorreu, bem como as medidas que foram ou serão adotadas para mitigar os riscos de um novo incidente.

8. PRIVACIDADE DOS DADOS

A segurança em computação contempla três princípios fundamentais: Confidencialidade, Integridade e Disponibilidade (CID), conforme Bishop [7], além das seguintes funções necessárias para o tratamento dos dados, informações e serviços de computação de acordo com Stallings [8]: autenticação, controle de acesso e irretratabilidade.

A confidencialidade trata de duas abordagens, a primeira com relação à confiabilidade dos dados, assegurando que a informação será manipulada somente por quem tem permissão, a segunda é com relação à privacidade, assegurando que os indivíduos possuam o controle apropriado sobre os seus dados, compreendendo a coleta, a armazenagem e a sua divulgação. A integridade busca assegurar que os indivíduos terão seus dados modificados ou alterados somente por quem tem o respectivo privilégio, a disponibilidade busca assegurar que os dados vão sempre estar disponíveis para serem utilizados pelos indivíduos [9].

Segundo Stallings [8], a autenticação numa comunicação garante que a mensagem está realmente sendo enviada pelo seu transmissor original, ou seja, assegura que não houve nenhuma alteração ou foi recebida por terceiros não autorizados. Controle de acesso: esse serviço controla quais usuários são autorizados e podem ter acesso a certos recursos do sistema. A irretratabilidade proporciona segurança contra o não-repúdio, isto é, impede que o receptor ou o transmissor neguem que enviaram ou receberam dados durante a comunicação.

Comumente, segurança e privacidade são tratados como sinônimos, sendo que a segurança engloba os mecanismos que podem ser empregados para assegurar que os requisitos de privacidade sejam atendidos, principalmente aos dados em formato eletrônico [9]. Segundo Brands [10], a definição mais aceita na literatura para a questão de privacidade do usuário com relação a sua informação e dados é: o direito de um indivíduo, grupo ou instituição de determinar por si próprio quando, como, para quem e em que nível as informações sobre si são comunicadas a outros. Esta relação entre privacidade e segurança vai além dos dados em formato eletrônico, abrangendo também o contexto físico dos dados, ou seja, quando existe a necessidade de se proteger a informação que se encontra em outras mídias. Neste sentido, a privacidade é mais complexa com relação ao tratamento de dados sensíveis.

Segundo Turn [11], os principais mecanismos para assegurar a proteção às informações pessoais são caracterizados como: legislativo, administrativo e técnico.

Na parte legislativa, temos o Marco Civil da Internet, lei n° 12.965/2014, que regula o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, e agora contamos também com a LGPD que apresenta um regime geral para o tratamento de dados pessoais.

Na parte administrativa, existem boas práticas e normas que se destinam a questão de privacidade e a segurança de dados digitais ou sistemas de armazenamento eletrônico, como as normas da família ISO/IEC 27000, sendo mais conhecidas as ISO 27001 (discutida posteriormente neste artigo) e ISO 27002.

Já na parte técnica, existe uma gama de ferramentas e soluções tecnológicas que com o intuito de garantir a privacidade dos dados, como o uso de soluções de criptografia e firewalls para controle de acesso, essas e algumas outras soluções serão discutidas no momento em que são aplicáveis durante a fase de do ciclo de vida dos dados em uma empresa.

9. O CICLO DE VIDA DOS DADOS

As empresas têm responsabilidades com os dados durante todo o período em que os possuem e os trata, formando assim um ciclo de vida dos dados que vai desde a coleta, passa pelas fases de retenção, processamento, compartilhamento, até sua eliminação. É de suma importância que as empresas identifiquem os ativos organizacionais envolvidos em cada uma das fases do ciclo de vida dos dados (base de dados, equipamentos, sistemas e entre outros), e adotem medidas de segurança em cada uma delas, tomando assim uma postura preventiva, visando mitigar os riscos de segurança envolvidos em cada uma delas.

O guia de boas práticas [2] define as fases do ciclo de vida dos dados e nós seguimos com algumas práticas de segurança relacionadas a elas, com o intuito de direcionar as empresas a atingirem conformidade com o que diz o art. 46: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito [1].

9.1 Coleta

O ciclo de vida dos dados se inicia com a coleta, sendo esta definida em [2] como: obtenção, recepção ou produção de dados pessoais independente do meio utilizado.

Durante a fase de coleta, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares [4].

Deve-se definir antecipadamente os mecanismos e procedimentos que os titulares dos dados deverão utilizar para consultar o conteúdo, a forma e a duração do tratamento dos seus dados pessoais, de maneira facilitada e gratuita (princípio do livre acesso), e garantir que quaisquer alterações quanto à finalidade especificada para o tratamento do dado; à forma ou à duração do tratamento; ao controlador responsável pelo dado; ou, ainda, à abrangência de compartilhamento sejam comunicadas ao titular [2].

Além disso, cabe à empresa obter o claro consentimento do usuário para o tratamento das informações coletadas. É importante que durante a fase de coleta haja uma restrição dos dados coletados, de forma que sejam coletados apenas o mínimo de informações necessárias para a finalidade de tratamento.

Outros pontos precisam estar claros e definidos também, sendo estes: 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. Todos estes procedimentos podem ser atingidos através de boas práticas instauradas pela governança dos controladores e operadores de informações coletadas [4].

Não deixar totalmente transparente ao titular todos esses pontos impede que os dados coletados sobre essas circunstâncias sejam tratados, pois desta forma estariam contrariando o que foi proposto no art.7 que apresenta as hipóteses de tratamento de dados, sendo assim, a empresa que não deixar claro aos titulares a quais dados serão coletados, a finalidade, o modo de tratamento, e a forma de exercício dos direitos dos titulares poderá sofrer com penalizações previstas no capítulo VIII da LGPD.

9.2 Retenção

A segunda fase do ciclo de dados é definida em [2] como: arquivamento ou armazenamento de dados pessoais independente do meio utilizado.

Esses dados podem estar armazenados em bases de dados, documentos, equipamentos ou sistemas. É preciso considerar também as unidades organizacionais responsáveis pelo armazenamento e guarda dos dados, bem como os locais físicos onde estão localizados os ativos que armazenam esses dados. Se o armazenamento for em "nuvem", por exemplo, é necessário considerar o serviço de armazenamento contratado e/ou utilizado [2]. Caso a empresa opte por terceirizar a responsabilidade do armazenamento, como soluções de armazenamento em nuvem, é necessário estar ciente da política de segurança da empresa contratada.

Durante a fase de retenção, existem uma série de medidas de segurança que devem ser levadas em consideração, pois existe o risco de ataques cibernéticos com o intuito de acessar essas informações de maneira ilegal e usa-las para obter algum tipo de vantagem contra seus detentores e/ou titulares.

9.2.1 Criptografia da informação

O uso de técnicas de criptografia é indicado para promover segurança sob os dados armazenados, uma vez que o conteúdo da informação armazenada é ininteligível para aqueles que não possuem a chave necessária para que seja realizado o processo inverso da criptografia a fim tornar o dado inteligível novamente.

Guimarães, em seu trabalho [5] apresenta a importância da criptografia: A criptografia computacional como se conhece protege o sistema quanto a ameaça de perda de confiabilidade, integridade, é utilizada para garantir:

• Sigilo: Somente os usuários autorizados têm acesso à informação.

• Integridade: Garantia que o usuário tem de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.

• Autenticação do usuário: Processo que permite ao sistema verificar se a pessoa com quem está se comunicando é de fato a pessoa que se alega ser.

• Autenticação do remetente: Processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem.

• Autenticação do destinatário: Consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário.

• Autenticação de atualidade: Consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

As técnicas de criptografia têm sua segurança avaliada com relação ao tamanho em bits da chave utilizada em conjunto com o algoritmo de cifragem, (este não precisa ser secreto), uma vez que o número de possibilidades para o valor da chave cresce exponencialmente na ordem de 2^n, onde n é o número de bits utilizados na chave.

Existe uma gama enorme de algoritmos com diferentes técnicas para cifragem dos dados, cabe a empresa mensurar o grau de sensibilidade das informações, e o custo computacional no momento de escolher o método de cifragem a ser seguido.

9.2.2 Anonimização e pseudonimização

Dado anonimizado é o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo [1]. A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta. A partir do momento em que o dado é considerado anonimizado, e não permite mais qualquer identificação do seu titular, esse dado sai do escopo da legislação, por não mais se tratar de um dado pessoal, conforme previsto no art. 12 da LGPD [2].

A pseudonimização é a técnica de tratar dados pessoais de uma forma em que os dados somente possam ser atribuídos a um titular de dados mediante a utilização de informações adicionais, não disponíveis a todos, desde que essas informações sejam mantidas em ambiente separado, controlado e seguro [2]. A criptografia por exemplo é uma pseudonimização, uma vez que em posse da chave utilizada na cifragem é possível obter a informação original, por isso a necessidade de que a chave utilizada seja mantida em segredo.

O processo de anonimização pode reduzir a informação original do conjunto de dados em certa medida, existem técnicas para proteção de dados por meio da anonimização (generalização, supressão, embaralhamento e perturbação), cada uma com um propósito específico que podem ser utilizadas e/ou combinadas, cabe a empresa decidir o *trade-off* entre a utilidade aceitável e a redução do risco de re-identificação dos dados.

O armazenamento de dados anonimizados acaba por se tornar uma forma de armazenamento mais segura do ponto de vista da legislação, pois uma vez que este tipo de dado não identifica um titular, não se trata mais de um dado pessoal e sai do escopo da LGPD, no caso de um incidente de segurança, estes dados vazados não podem identificar os titulares. Como existe um custo computacional, muitas vezes associado a um custo financeiro também para a utilização de técnicas de anonimização, sugerimos que as empresas utilizem tais técnicas ao menos em dados sensíveis, e dados de menores de idade, visto que incidentes de segurança que envolvem estes tipos de dados serão considerados mais graves, sofrendo maiores sanções da ANPD.

9.2.3 Outras medidas de segurança

Além da criptografia e da anonimização dos dados armazenados, existem uma série de outras práticas de segurança a serem adotadas na fase de retenção dos dados, as quais sugerimos, que ajudam na garantia de privacidade e consequentemente na adequação à LGPD.

• Controle de acesso: Uma vez que os dados estejam armazenados, é necessário que apenas pessoas autorizadas possuam acesso a eles, uma forma de promover isso é por meio de autenticação de usuários com login e senha, adoção de políticas de senhas seguras com grande quantidade e variedade de caracteres como presença de dígitos e caracteres especiais, mecanismos de rejeição de senhas utilizadas anteriormente e de renovação periódica ajudam a promover segurança contra violação deste tipo de autenticação. Outro ponto é a autenticação de dois fatores, em que um outro meio de autenticação é associado ao login e senha, como um código pin enviado ao celular do usuário ou uso de dispositivos de biometria para garantir que o usuário que está tentando acessar o sistema é quem realmente diz ser e que não teve suas informações de login obtidas de maneira ilegal. Além dos acessos aos sistemas, é necessário também uma segurança física do local onde os dados são armazenados, de modo que o acesso ao local físico seja controlado e restrito aos funcionários.

• Visão de dados: É importante restringir os acessos dos funcionários aos dados da empresa, de modo que estes tenham visibilidade apenas das informações que são essenciais para o seu trabalho, mitigando assim os riscos de acesso indevido e/ou perda de dados da empresa.

• Cópias de segurança: Uma medida de prevenção eficaz contra a perda dos dados armazenados de uma empresa é manter uma cópia desses dados em uma outra localidade. Esta redundância das informações pode ser de extrema importância em diversas situações como em caso do comprometimento dos dados originais por meio de um ataque criminoso, ou pela ocorrência de desastres naturais ou não no local físico do armazenamento dos dados. Por essas e outras possibilidades, manter uma cópia dos dados em um local físico diferente do original é de extrema importância. Cabe à empresa decidir quais dados devem ser replicados e com que frequência visto que existe um custo associado ao armazenamento.

9.3 Processamento

A terceira fase do ciclo de vida dos dados, o processamento, é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais retidos pelo controlador. É preciso identificar as pessoas (papéis organizacionais), unidades organizacionais e equipamentos envolvidos nesse tratamento.

É importante que durante a fase de processamento as empresas mantenham seus sistemas envolvidos no processamento, atualizados com os pacotes de atualizações mais recentes, visto que estes podem corrigir eventuais vulnerabilidades dos sistemas.

Uma ferramenta importante para registro de processamentos e para auditorias são os logs. Arquivos de logs podem registrar os eventos relevantes de segurança da informação, contendo a identificação do usuário, a natureza do evento, a data, hora, e os identificadores de quais informações estão sendo tratadas, de modo que seja possível identificar a origem do evento.

9.4 Compartilhamento

Esta fase envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais [2].

Durante a fase de compartilhamento é necessário saber quais sistemas e equipamentos são usados para transmitir, exibir ou divulgar os dados pessoais. Além de ter uma preocupação com medidas de segurança da informação nos equipamentos e sistemas envolvidos na fase de compartilhamento para que haja um ambiente seguro de troca de dados, a empresa deve se certificar que os dados estão sendo compartilhados unicamente com seus titulares, ou com outros controladores desde que haja um consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas em lei.

9.5 Eliminação

Por fim, a eliminação é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados. Deve-se avaliar os ativos que armazenam os dados pessoais que possam ser objeto de solicitação de eliminação de dados a pedido do titular ou descarte nos casos necessários ao negócio da instituição. Os dados pessoais a serem eliminados podem estar armazenados em ativos relacionados com bases de dados, documentos, equipamentos ou sistemas. Se a eliminação do dado pessoal ou descarte do ativo tiver relação com solução em "nuvem", por exemplo, é preciso considerar o serviço de armazenamento contratado ou utilizado [2].

Nos termos da LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses [2]:

• Exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;

• Fim do período de tratamento;

• Revogação do consentimento ou a pedido do titular, resguardado o interesse público;

• Determinação da autoridade nacional em face de violação do disposto na lei.

Na incidência de qualquer uma das hipóteses acima, a lei determina que os dados sejam eliminados, a não ser nos casos em que [2]:

• Remanesça o cumprimento de obrigação legal ou regulatória pelo controlador;

• Sejam necessários para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;

• Ocorra a transferência a terceiro, desde que respeitados os requisitos de tratamento dispostos em lei;

• Seja utilizado exclusivamente pelo controlador, vedado seu acesso por terceiro, e desde que anonimizados.

É importante que as empresas tenham uma política de eliminação de dados pessoais para as hipóteses de fim de tratamento citadas acima, uma vez que além de estarem de acordo com a lei, estarão evitando um gasto excessivo com custo de armazenamento, e gerenciamento de dados pessoais, além de estarem minimizando riscos de roubo de informações.

10. PADRÕES PARA CONTROLES DE SEGURANÇA DA INFORMAÇÃO

A privacidade deve ser protegida continuamente em todo o domínio e ao longo do ciclo de vida do tratamento dos dados em questão. O princípio "Segurança" tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade. As instituições devem assumir a responsabilidade pela segurança dos dados pessoais, geralmente proporcional ao grau de sensibilidade, durante todo o ciclo de tratamento, consistente com os padrões que foram definidos por organismos reconhecidos de desenvolvimento de padrões. Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro [2].

10.1 A Política de Segurança da Informação e a ISO 27.001

A Política de Segurança da Informação (PSI) é um documento que precisa possuir um conjunto de diretrizes, técnicas e procedimentos, que necessitam ser transmitidos a todos os colaboradores, sendo assim analisado, averiguado e revisto criteriosamente em períodos constantes ou no caso de haver necessidade de mudanças vigentes. Para que seja elaborada a PSI é necessário ter a importância da NBR ISO/27001:2013 pois é uma norma de diretrizes de boas práticas para o gerenciamento da segurança da informação, na qual pode ser identificada as melhores técnicas para principiar, executar, preservar e aprimorar o gerenciamento da segurança da informação em uma empresa. A norma ISO 27001 designa instruções para se estabelecer, guardar, preservar e aprimorar o gerenciamento de segurança da informação dentro de uma corporação [12].

Aprovada e traduzida e pela Associação Brasileira de Normas Técnicas (ABNT) e transformada em uma Norma Brasileira (NBR) a ISO 27001 apresenta os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de gestão da Segurança da Informação (SGSI), bem como os requisitos para avaliação e tratamento de riscos de segurança da informação, sempre com o foco nas necessidades da organização.

Em seu trabalho [12] Pereira *et al* apresentam doze pontos de comparação entre a LGPD e a ISO 27001, para adotar o padrão ISO e entrarem em conformidade com a LGPD as empresas devem:

• Adotar políticas de segurança da informação, prover orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes [13]. A Política de segurança deve estar disponível com todas as informações documentadas, ser comunicada dentro da organização e estar disponível para todas as partes interessadas. Este ponto está de acordo com o que diz o art. 50 da LGPD [1] que trata das boas práticas e da governança.

• Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização [13]. Segundo a LGPD as empresas devem adotar auditoria interna e externa de dados, em intervalos planejados, para estar em conformidade com as regras da lei e as regras da própria organização, de acordo com a ISO 27001 as empresas devem [13]:

a) planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores;

b) definir os critérios e o escopo da auditoria, para cada auditoria;

c) selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria;

d) assegurar que os resultados das auditorias são relatados para a direção pertinente;

e) reter a informação documentada como evidência dos programas da auditoria e dos resultados da auditoria.

Além de adotar auditoria dos seus dados, as empresas também devem manter contato com as autoridades relevantes, neste caso a ANPD.

• Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos. Segundo a LGPD os ativos da organização são todos os dados pessoais, e isso possibilitará que as empresas compreendam quais dados pessoais estão inclusos e onde registrá-los, por qual período, qual a sua procedência e quem tem acesso, que são todos os requisitos citados na lei.

• Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização. De acordo com a ISO deve ser desenvolvido e implementado um esquema para a classificação dos ativos que nesse caso serão os dados. A exemplo de dados que precisam de uma proteção maior citamos os dados pessoais sensíveis e também os dados referentes a menores de idade.

• Limitar o acesso à informação e aos recursos de processamento da informação. Deve ser estabelecido os controles para acesso da informação, a informação deve ser documentada e analisada de acordo com os requisitos de segurança, da empresa, do negócio e da LGPD.

• Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

• Tornar os usuários responsáveis pela proteção das suas informações de autenticação. De acordo com a ISO a empresa deve orientar seus usuários a maneira como devem seguir as práticas da organização e segundo a LGPD os agentes de tratamento de dados só não serão responsabilizados se provarem que o dano causado é decorrente da culpa do próprio titular ou de terceiros.

• Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas. Deve ser estabelecido políticas e procedimentos para o controle da transferência de dados dentro ou fora da empresa, as empresas internacionais que solicitarem informações dos dados de clientes, devem ter normas ou legislações que estejam de acordo com todos os requisitos de transferência internacional de dados citadas LGPD.

• Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas. De acordo com a LGPD, as empresas precisam utilizar sistemas mais estruturados para atender os requisitos de segurança dos dados e precisarão investir em tecnologia para garantir a integridade dos mesmos, com requisitos relacionados na legislação ou melhorias nos sistemas que já possuem.

• Garantir a proteção dos ativos da organização que são acessados pelos fornecedores. As empresas devem garantir que as informações passadas para os fornecedores estejam de acordo com os requisitos da lei para a proteção dos dados e privacidade do titular, de acordo com a ISO deve ser feito acordos e devem ser documentados para mitigar os riscos associados com o acesso de fornecedores.

• Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação. Para uma melhor segurança dos dados, as empresas devem realizar avaliações como intervalos de tempo, de forma planejada, adotando medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados, ou acidentais, ou ilícitas, de qualquer que seja a forma de tratamento dos dados. A ISO orienta a comunicação com autoridades responsáveis, procedimentos para agilidades nas respostas, que os funcionários sejam instruídos a notificar fragilidades nos sistemas, que o evento seja classificado para uma melhor avaliação dos danos, que as autoridades sejam notificadas de acordo com procedimentos documentados e que a empresa deve aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações.

• Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança. As empresas devem estar atentas ao funcionamento da ANPD e ao que for imposto por ela para que não haja violações de obrigações legais.

Embora a ISO 27001 cubra 80% da LGPD, segundo Pereira et al [12], empresas que possuem a certificação ISO 27001 já podem se considerar nos conformes da LGPD. Existem uma série de outras normas ISO/ABNT que podem ser seguidas e adotadas como boas práticas em segurança da informação como ABNT NBR ISO/IEC 27002: 2013 código de prática para controles de segurança da informação, a ABNT NBR ISO/IEC 27005:2019 gestão de riscos de segurança da informação, ou ainda ABNT NBR ISO/IEC 31000:2018 que trata de diretrizes para gestão de riscos.

11. A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Proposta no capítulo IX da LGPD, a ANPD é o órgão federal responsável por operacionalizar a parte de fiscalização, bem como definir, quando necessário, questões técnicas mínimas a serem adotadas pelos agentes de tratamento de dados, ANPD também tem a função de informar sobre os direitos dos titulares, bem como estimular o entendimento das normas pelas empresas que fazem uso dos dados e informações pessoais. A ANPD possui autonomia técnica e decisória para fiscalizar e elaborar diretrizes e normas relacionadas à proteção, coleta, uso, armazenamento e distribuição de dados pessoais dos cidadãos brasileiros.

A ANPD poderá aplicar sanções em caso de violação da legislação a partir de agosto de 2021. As penalidades variam de acordo com o caso e após processo administrativo que fará a análise da ocorrência, são aplicadas: advertências simples, multas de 2% do valor do faturamento da empresa ou grupo no último exercício, bloqueio ou exclusão dos dados envolvidos na ocorrência e suspensão ou proibição do acesso ao tratamento de dados pessoais [14].

A criação de uma autoridade independente é necessária para que empresas que têm acesso a informações pessoais cumpram a legislação e possam ser auditadas nos casos em que não observarem o devido tratamento destes dados. É a ANPD que irá fazer cumprir o que foi estabelecido pela LGPD, em casos de vazamento de dados, acessos indevidos e outros casos de descumprimento da lei, é a ANPD quem irá analisar e autuar os culpados do ocorrido, podendo também ser contatada pelos titulares dos dados caso estes não tenham seus direitos previstos em lei atendidos pelos controladores dos dados.

12. CONCLUSÃO

A LGPD estabeleceu um amparo legal para o tratamento de dados pessoais, trazendo uma série de direitos aos titulares dos dados e consequentemente obrigações às empresas que coletam e tratam

esses dados, visto a proximidade do início da aplicação de sanções em casos de descumprimento da lei por parte da ANPD, as empresas precisam rapidamente entrarem em conformidade com o que foi estabelecido pela LGPD, e isso requer rever todo o processo do negócio para que haja uma adequação para a proteção dos dados, adotando um comportamento preventivo quanto a segurança do tratamento de dados, desde sua aquisição até sua eliminação.

Até a data da publicação deste artigo, está em análise uma proposta elaborada pelo Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae), com a contribuição de outras 15 entidades, enviada pelo ministério da economia à ANPD, que trata da regulamentação de um tratamento diferenciado para aplicação da LGPD às Micro e Pequenas Empresas (MPEs). Dentre as propostas, estão a dispensa das seguintes obrigações: indicar uma pessoa exclusivamente responsável pelo tratamento de dados da empresa, manter registro das operações de tratamento e elaborar relatórios periódicos de impactos à proteção de dados, entre outras. O Sebrae também contribuiu com sugestões para o processo de aplicação de multas, propondo redução de multa em 90% para os MEI (microempreendedores individuais) e 50% para as MPEs. Os termos valem para os empreendedores que estejam adimplentes com suas obrigações financeiras, hajam de boa-fé e não apresentem comportamentos que dificultem a fiscalização.

A proposta encaminhada à ANPD é justificada pelo fato de muitas micro e pequenas empresas funcionarem com número reduzido de pessoal, às vezes por um único funcionário no caso dos MEI, tal proposta reduz obrigações e flexibiliza penalizações previstas pela LGPD.

Caso a organização que precisa entrar em conformidade com a LGPD se enquadre como uma micro ou pequena empresa ou ainda como MEI, é importante que esta verifique junto a ANPD (https://www.gov.br/anpd/pt-br), se a proposta para regulamentação da aplicação da LPGD para MEIs foi oficialmente regulamentada, e quais as obrigações que estes pequenos negócios estão legalmente dispensados, até que haja a regulamentação é importante que estes e demais negócios iniciem seu processo de adequação à lei, visto que este pode ser um processo demorado e que envolve planejamento para gerenciamento de tempo, ativos e custos associados.

13. REFERÊNCIAS

[1] BRASIL. DECRETO N° 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais, Brasília - DF, ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em 11 maio de 2021.

[2] Cravo, Victor *et al*. 2020. *GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).* Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf Acesso em 11 maio de 2021.

[3] Junior, Eric A. da C. 2020. *Análise de conformidade de processos de negócios em relação a LGPD*. Recife - PE. Disponível em: https://www.cin.ufpe.br/~tg/2020-3/TG_SI/tg_eacj.pdf Acesso em 11 maio de 2021.

[4] Oliveira, Nairobi S. de *et al*. 2019. *Segurança da Informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD).* São Leopoldo - RS. Disponível em: https://www.seer.ufrgs.br/reic/article/view/88790/55009 Acesso em 11 maio de 2021.

[5] Guimarães, Carla R. 2001. *Criptografia para Segurança de Dados*. Uberlândia. Disponível em: http://www.computacao.unitri.edu.br/downloads/monografia/79431146079328.pdf Acesso em 11 maio de 2021.

[6] Gov.br. 2021. *Comunicação de incidentes de segurança.* Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Acesso em 11 maio de 2021.

[7] Bishop, Matt. *Computer Security: Art and Science.* Upper Saddle River: Pearson Education, 2003.

[8] Stallings, William. *Cryptography and Network Security: Principles and Practice.* Upper Saddle River: Prentice Hall, 1999.

[9] Rojas, Marco A. T.; Medeiros, Jucelio K. *Avaliação da adequação de Instituto Federal à Lei Geral de Proteção de Dados Pessoais.* Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação, [S.l.], v. 1, n. 13, jan. 2021. ISSN 2446-7634. Disponível em: https://revistas.setrem.com.br/index.php/reabtic/article/view/391 Acesso em 11 maio de 2021.

[10] Brands, Stefan. A. 2000. *Rethinking public key infrastructures and digital certificates: building in privacy.* The MIT Press. Montreal.

[11] Turn, R. *Security and privacy requirements in computing*. In Proceedings of 1986 ACM Fall joint computer conference (ACM '86). IEEE Computer Society Press, Los Alamitos, CA, USA, 1106-1114.

[12] Pereira da Rocha Camila *et al. Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD*. Belém-PA. Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará, [S.l.], v. 2, n. 3, p. 78-97, ago. 2019. ISSN 2595-8798. Disponível em: http://www.revistasfap.com/ojs3/index.php/tic/article/view/285 Acesso em 11 maio de 2021.

[13] Associação Brasileira De Normas Técnicas. NBR ISO/IEC 27001. 2013. *Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.* Rio de Janeiro - RJ.

[14] Tecnoblog. 2021. *O que é ANPD? [Autoridade Nacional de Proteção de Dados].* Disponível em: https://tecnoblog.net/409033/o-que-e-anpd-autoridade-nacional-de-protecao-de-dados/ Acesso em 11 maio de 2021.