Conteúdo Jurídico
www.conteudojuridico.com.br

PEQUENAS E MÉDIAS EMPRESAS E A ADEQUAÇÃO A LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL, ALIADA AS BOAS PRÁTICAS BASEADAS NA *GENERAL DATA PROTECTION REGULATION* DA UNIÃO EUROPEIA

ANDREW CARL DINIZ BENZAQUEN: Acadêmico e Pesquisador de Direito (Digital). Cientista de dados em formação. Analista de TI (Governança, Processos e Compliance).

NATASHA DE SOUZA MENDONÇA[1]

(coautora)

DR. ALLAN DUARTE MILAGRES LOPES

(orientador)

Resumo: O presente artigo relata o panorama da Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD) e sobre a Medida Provisória nº 959, de 2020 que tinha a intenção de postergar sua vacância para 2021. O objetivo deste texto é elucidar a necessidade da regulamentação da proteção de dados no Brasil e como se dará a sua adequação pelas Micros, Pequenas e Médio Empresas, assim como as consequências jurídicas de possíveis vazamentos de dados pessoais por estas. Deu-se ênfase especial nos passos para adequação jurídica e das boas práticas de segurança da informação para as Pequenas e Médias Empresas, neste diploma legal, partindo das experiências na Europa com a Regulamento Geral sobre a Proteção de Dados – GDPR de 2016.

Palavra Chaves: LGDP, GDPR, DPO, Encarregado de Dados, Controlador, Proteção de dados, Vazamento de dados, Dados Sensíveis, Modelo de Desenho de Privacidade.

Abstract: This article reports the panorama of Law No. 13,709, of August 14, 2018, here called the General Law for the Protection of Personal Data (GPPD) and on Provisional Measure No. 959, of 2020 that postpones its vacancy to 2021. The objective from this text it is necessary to elucidate the need for data protection regulation in Brazil and how it will be adapted by Micro, Small and Medium Enterprises as well as the legal consequences of possible leaks of personal data by them. Particular emphasis was placed on the steps towards legal adequacy and good information security practices for SMEs (Small and medium-sized enterprises) in this legal diploma, building on experiences in Europe with the 2016 General Data Protection Regulation - GDPR.

Keywords: GPPD, GDPR, DPO, Data Controller, Controller, Data Protection, Data leakage, Sensitive Data, Privacy Design Framework.

1 Acadêmicos do 10° período do curso de Direito do Centro Universitário UNA Contagem.

elencados. 4. Quem pode tratar os dados das PMEs? 4.1 As certificações de institutos internacionais para profissionais no Brasil. **5. Como adequar as PMEs a LGPD – Boas Práticas de Proteção de dados na Europa.** 5.1.1 *Privacy by Design.* 5.1.2 *Privacy by Default.* 5.1.3 – Os princípios do *Privacy by Design.* 5.1.3.1. Proativo, não reativo. Prevenir, não remediar. 5.1.3.2. Privacidade por padrão. 5.1.3.3 Privacidade embutida no design. 5.1.3.4. Total funcionalidade. 5.1.3.5 Segurança ponta a ponta. 5.1.3.6 Visibilidade e Transparência. 5.1.3.7 Respeito pela privacidade do usuário. 5.2 Ciclo de vida dos Dados na LGPD. 5.3 Semelhanças e diferenças entre LGPD X GDPR. 5.4 Documentos que devem ser criados como boas práticas de adequação a proteção da privacidade de dados. **6. Consequências jurídicas da não adequação da LGPD das PMEs. 7. Potencial aumento de demandas judiciais. 8. O que as PME's devem fazer em caso de vazamento de dados. 9. Conclusão. 10. Referências bibliográficas**

1.INTRODUÇÃO

É evidente como o universo digital vem, cada vez mais, influenciando o comportamento da sociedade e por mais abstrato que pareça, as empresas devem começar a considerá-lo como uma ferramenta que além de trazer praticidade requer cuidados. Nesse cenário de evolução tecnológica surge o Direito Digital, que conecta a ciência com o mundo jurídico para nortear empresas, profissionais e consumidores para mitigar incidentes e transmitir credibilidade em algo que ainda gera muita insegurança.

Outrossim, inspirada na *General Data Protection Regulation* - GDPR, a Lei Geral de Proteção de Dados - LGPD surge como resposta aos brasileiros e prevê obrigações sobre tratamentos de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica – seja qual for seu porte – de direito público ou privado, com o intuito de proteger direitos fundamentais de liberdade e de privacidade, atualizando conceitos que antes eram esparsos na legislação pátria ou eram interpretados de maneira análoga a outros institutos.

1.1 Panorama da Lei Geral de Proteção de dados na era Covid19

O avanço jurídico com a criação da LGPD, a sanção parcial do presidente da República ao Projeto de Lei nº 1.179/20 – a qual dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado no período da pandemia da Covid-19 – posterga as sanções administrativas elencadas pela LGPDpara 2021, o que resulta em insegurança jurídica, posto que a lei entra em vigor sem a devida regulamentação da ANPD – Autoridade Nacional de Proteção de Dados.

1.2 Protelação da Lei Geral de proteção de dados

No último dia 26 de agosto de 2020, o Senado impõe uma derrota ao Governo de Jair Messias Bolsonaro, que havia defendido no Congresso sobre a postergação da eficácia da LGPD para maio de 2021. No primeiro momento, os líderes do Congresso acordaram o adiamento para 31 de dezembro de 2020, entretanto, no afligir das eleições municipais de 2020 e o acirramento da polarização política, a crise econômica e sanitária, cumuladas com a perda de popularidade do governo Bolsonaro, fez com que o Senado retomasse a discussão, sendo decisivo e não aceitando mais a postergação da LGPD para 2021, tampouco para dezembro de 2020. Por conseguinte, a MP/959 não foi convertida em lei, e a LGPD entrou em vigor no Brasil no último dia 18 de setembro de 2020. No dia 26 de agosto, foi publicado o Decreto nº 10.474/2020, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados – ANPD, remanejando e transformando cargos em comissão e funções de confiança, sem a prorrogação da LGPD, o que implica em uma derrota ao governo.

Em 15 de outubro de 2020, Bolsonaro nomeou cinco nomes para compor a Autoridade Nacional de Proteção de Dados – ANPD, sendo destes cinco, três militares e duas advogadas civilistas representando o Direito Privado, indicações contestadas por alguns setores em virtude dos currículos técnicos, porém militares na maioria dos membros, o que pode influenciar e tirar a autonomia que a Autoridade Nacional de Proteção de dados, tendo em vista que a composição é notoriamente ligada ao Presidente Jair Messias Bolsonaro.

Os impactos e incertezas econômicas geradas pela pandemia da Covid-19 nos processos de adequação são compartilhados por todo mundo. Na Califórnia, apesar da lei de proteção de dados já estar em vigor, a fiscalização – ou *enforcement* – ainda está suspensa e instituições de diversos setores já pressionam o governo para manter essa suspensão; uma tendência que estava sendo seguida pelo Brasil.

Ressalta-se que a alteração da regulamentação da LGPD, embora tardia e figurada apenas no campo teórico, inclui o Brasil no rol de países que têm legislação específica sobre privacidade de dados, cumprindo um dos requisitos para participar da Organização para a Cooperação e Desenvolvimento Econômico – OCDE. Portanto, faz-se necessária a ANPD para regulamentação da norma, evitando insegurança jurídica e prejudicialidade em casos específicos. Em um cenário que não se tenha a ANPD constituída, cabe as empresas tirar proveito deste "*delayed enforcement*" estabelecido com o suposto adiamento do órgão regulador e usar a hermenêutica para o que for mais conivente.

Ademais, será exigido da ANPD, do poder judiciário e dos controladores uma adaptação voltada não só para as práticas de privacidade relacionada à Tecnologia da Informação, mas também ao risco de judicialização de demandas em massa acerca do tema, transformando o judiciário em uma "indústria do dano moral", com casos que poderiam ser solucionados extrajudicialmente com as empresas ou administrativamente com a ANPD. Vale ressaltar que consta em tramitação no congresso a PEC 17/2019[2] que visa fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Mais a mais, embora anseia-se que a partir de outubro de 2020, muitas empresas tenham recursos para os projetos de adequação à LGPD, fato é que, é difícil imaginar que os orçamentos sejam recuperados após a pandemia – ainda sem perspectiva de controle – e atinjam sua integralidade, o que mantém o Brasil em baixo nível de proteção se comparado aos padrões internacionais, dificultando o relacionamento com fornecedores de outros países.

Partindo deste cenário, trazemos à baila a necessidade de adequação das PME's para a Lei geral de Proteção de Dados, para que acompanhem a competitividade do mercado, com práticas e ferramentas acessíveis que, sem comprometer o seu orçamento, tratando com seriedade a privacidade de dados.

Este artigo é norteado pelas orientações de boas práticas de proteção de dados à Europa, que teve a GDPR aprovada em 2016 e regulamentada em 2018, fomentando estudos e modelos de gestão de dados adequados à GDPR – Legislação que foi base para construção da nossa LGPD.

---

2 Texto integral da Proposta de Emenda à Constituição 17, que visa alterar Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Endereço para o texto da PEC 17: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757

Explanaremos neste artigo como as PME's podem se adequar à LGPD utilizando o modelo de desenho de privacidade da PhD Canadense *Ann Cavoukian*, modelo que se tornou referência para as empresas. Abordaremos também quais os documentos necessários para aplicação deste *framework* e as principais semelhanças e diferenças entre a GDPR e a LGPD.

2.A importância das PMEs para o Brasil

Em consonância com a Lei Complementar n° 123, de 14 de dezembro de 2006, conhecida como Lei Geral da Micro e Pequena Empresa, é considerada uma microempresa a sociedade empresária ou simples, a empresa individual de responsabilidade limitada e o empresário com receita bruta anual de R$360 mil reais. Quando a renda bruta anual for superior a este valor e inferior a R$ 3,6 milhões, a entidade será considerada uma pequena empresa.

De acordo com o Conselho Federal da Administração – CFA[3], as micros e pequenas empresas têm um papel econômico fundamental no Brasil. Além de representarem a maioria de todos os negócios formais do país, são responsáveis por uma grande fatia do faturamento de todas as empresas brasileiras, contratando mais da metade da mão de obra formal. Segundo o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), elas já são as principais geradoras de riqueza no país. As PME's respondem por 53,4% do Produto Interno Bruto (PIB) do comércio e, na indústria e no setor de serviços, a participação delas também é relevante – 22,5% e 36,3%, respectivamente. Representam também 27% do PIB, 52% dos empregos com carteira assinada, 40% dos salários pagos, 8,9 milhões de microempresas. Ratificando a pesquisa divulgada pelo Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), a participação das micro e pequenas empresas brasileiras somadas representam 27% de todo o Produto Interno Bruto (PIB) do Brasil. Ressalta-se que, se compararmos com números de décadas passadas, veremos que a participação das micro e pequenas empresas na economia brasileira cresce acentuadamente. Em 1985, representavam 21% do PIB. Já em 2001, 23,2%. Em termos de valores absolutos, de 2001 a 2011, o faturamento das micro e pequenas empresas saltou de R$ 144 bilhões para R$ 599 bilhões, em valores da época. Nesse sentindo, foi o fator decisivo para que este trabalho fosse recortado para PME's. Se considerarmos a participação no mercado de trabalho, verificamos que as micro e pequenas empresas têm uma importância ainda maior na economia brasileira, posto que os salários pagos por elas respondem por 40% da massa salarial brasileira, como foi informado em pesquisa realizada pelo SEBRAE.

De acordo com o Luiz Barretto, presidente do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas, em entrevista ao portal do SEBRAE[4], o crescimento das micro e pequenas empresas na última década é motivado pelo melhor ambiente de negócios, como a criação dos Supersimples (que reduziu e unificou impostos para os pequenos negócios), o aumento da escolaridade dos brasileiros e o incremento do mercado consumidor na classe média. Além disso, ele considera que as pessoas estão abrindo pequenos negócios por acreditar no empreendedorismo, não apenas por falta de empregos, como antigamente.

> *"Esses três fatores têm motivado o brasileiro a empreender por oportunidade e não mais por necessidade. Antes as pessoas abriam um negócio próprio quando não encontravam emprego. Hoje, de sete a cada 10 pessoas iniciam*

3 O Conselho Federal de Administração informa a importância das Pequenas e Médias Empresas para nossa economia, em especial o impacto no Produto Interno Bruto (PIB), estudo publicado no capítulo de ancoras do portal do Conselho: https://cfa.org.br/ancoras-da-economia/

4 Segundo artigo publicado no portal do SEBRAE as Pequenas e Médias Empresas tem um crescimento evidente nos últimos anos devido a introdução do Supersimples, artigo pode ser visto em: https://sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/micro-e-pequenas-empresas-geram-27-do-pib-do-brasil,ad0fc70646467410VgnVCM2000003c74010aRCRD

> *um empreendimento por identificar uma demanda no mercado, o que gera empresas mais planejadas e com melhores chances de crescer", avalia o presidente do Sebrae, Luiz Eduardo Pereira Barretto Filho.*

De acordo com o levantamento do Sebrae, são mais de 8,9 milhões de micro e pequenas empresas no Brasil. O último levantamento do IBGE (Instituto Brasileiro de Geografia e Estatística) indicou que os pequenos negócios representam 99% dos estabelecimentos formais do país.

Em contrapartida ao crescimento informado em linhas volvidas, é inegável que os pequenos empreendimentos enfrentam dificuldade para se estabelecerem nos mercados nacionais, tendo em vista a competitividade causada pela livre concorrência da atividade empresarial. Por isso, na mesma base destes argumentos, devemos direcionar as nossas discussões sobre como promover a prosperidade empresarial, oferecendo aos microempresários e empresários de pequeno porte condições necessárias ao seu desenvolvimento, sem que desrespeitemos a liberdade em que a economia está pautada.

Atentos a esta realidade, devemos analisar um plano especial de adequação à LGPD para esta categoria que enfrentará dificuldades maiores se considerarmos somente o capital que dispõem, sendo necessário diretrizes que corrijam essa desvantagem econômica e que dê oportunidade de crescimento também as pequenas e médias empresas.

2.1 Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados – ANPD, foi definitivamente criada após a sanção da MP 869/2018, convertida na Lei 13.853/2019. Em sinergia com a compreensão disposta no art. 5º, XIX, da LGPD, a Autoridade Nacional é o órgão da Administração Pública encarregado por zelar, implementar e fiscalizar o cumprimento da LGPD integralmente no Brasil. Entretanto, esse conceito não é suficiente para entender a extensão de sua atuação.

Há muitos questionamentos sobre qual é papel da ANPD, que no último dia 15 de outubro de 2020, teve cinco membros nomeados pelo Presidente Jair Messias Bolsonaro. Esses nomes foram submetidos a sabatina à Comissão de Infraestrutura do Senado, sendo todos foram aprovados por unanimidade. No entanto, as nomeações provocaram um desconforto em parte dos setores – majoritariamente opositores ao governo Bolsonaro – que defendem a ANPD funcionando. Isso porque, três nomeados são militares notoriamente ligados ao presidente, o que pode causar interferência e ferir a autonomia desejada, algo que já tem sido observado nas recentes crises envolvendo o presidente, como por exemplo a do o ex-Ministro de Segurança e a Polícia Federal, Sergio Moro.

É sabido que a regulamentação é essencial para a efetiva aplicação das normas de privacidade e proteção de dados, entretanto há de se ponderar se tais nomeações não comprometem a autonomia da Autoridade Nacional de Privacidade de Dados. Considerando que a LGPD é uma norma principiológica[5], conforme seu artigo 6°, ou seja, uma norma que

fixa preceitos gerais, com princípios a serem seguidos, um órgão que estabeleça bases e diretrizes gerais para o seu cumprimento, contribui para maior eficiência da sua implementação.

---

5 O conceito principiológico da LGPD pode ser observado no seu artigo 6°e foi amplamente discutido no VIII Workshop de Privacidade e Proteção de Dados Pessoais - Princípios na LGPD da OAB Contagem, podendo ainda ser acessado seu conteúdo através do endereço: https://www.youtube.com/watch?v=VRcSDRy4Ips&ab_channel=OABContagem

Com a ANPD atuante, além de fiscalização e aplicação de sanções, haverá regulamentações e procedimentos sobre proteção de dados pessoais e privacidade, para que os agentes de tratamento e os titulares de dados compreendam o alcance da norma.

Sua composição foi regulada pelo Decreto nº 10.474, de 26 de agosto 2020, que aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados, remanejando e transformando cargos em comissão e funções de confiança. Os cinco nomes nomeados pelo chefe de estado, foram sabatinados pela Comissão de Infraestrutura do Senado, conforme estabelece a nossa Constituição em seu artigo 52, que define as competências do Senado, reza-se:

> *"Art. 52. Compete privativamente ao Senado Federal - III - aprovar previamente, por voto secreto, após arguição pública, a escolha de - f) titulares de outros cargos que a lei determinar;"*

Ressalta-se ainda que a criação da ANPD sinaliza aos países que também estão se adequando ao novo paradigma da privacidade de dados pessoais, que o Brasil está comprometido na adoção de medidas práticas, visando a proteção dos dados pessoais, o que pode contribuir para a segurança e crescimento das negociações internacionais em diversos segmentos.

Embora ainda exista uma visão que a ANPD atuará apenas como a "pardal", aplicando multas milionárias aos agentes de tratamento, é necessário esclarecer que a sua atuação não será apenas direcionada às sanções. A ANPD terá competência normativa, deliberativa, fiscalizadora e sancionatória, tendo como principal função zelar pela proteção de dados pessoais.

O órgão será responsável pela elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, com a finalidade de nortear os agentes de tratamento para que atuem em conformidade com as normas. É importante, inclusive, que as empresas trabalhem consoante não só com as normas, mas em parceria ao órgão regulamentador, para que evitem a judicialização de demandas que podem ser solucionadas extrajudicialmente ou administrativamente.

Nesse sentido, as sanções devem ser vistas como a última opção, quando houver violação dolosa ou negligente. Em um primeiro momento, é essencial que haja mecanismos simplificados para registro de reclamações e estímulos para adoção de serviços que facilitem o controle pelo operador e pelo titular. Compete à ANPD promover aos interessados o conhecimento das normas, primando pela boa-fé e conscientizando de maneira simples, sobretudo as PME's, com diálogo e cooperação, para que haja um maior engajamento no mercado e a lei não vire somente suprimento para a "indústria do dano moral".

Há uma grande expectativa para que a ANPD seja um suporte àquelas empresas que estão no processo de adequação à lei. A lei dispõe que será assegurada a autonomia técnica e decisória à ANPD, características necessárias para uma legítima atuação, de forma a garantir tanto aos agentes de tratamento quantos aos titulares, decisões e orientações isentas a respeito dos impactos da norma.

Um dos pontos mais importantes além da atuação instrutiva, é o dever de atuação fiscalizatória, que terá grande impacto para a implementação da LGPD. A Autoridade Nacional será responsável por fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso. Ressalta-se que a aplicação das sanções não será imediata,

limitando-se à multa de R$50.000.000,00, mas podendo ser aplicadas advertências, com indicação de prazo para adoção de medidas corretivas e multas simples de até 2% do faturamento no seu último exercício, excluídos os tributos.

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os critérios da LGPD. Destaca-se que, da mesma forma que a ANPD observará as peculiaridades de cada caso, o processo de *compliance* à LGPD também deverá ser personalizado para cada empresa, não sendo possível uma receita genérica para todos os segmentos.

Em suma, o bem-estar da economia não pode sobrepujar as considerações de justiça. Portanto, precisamos nos perguntar em quais condições as pessoas são livres para fazer suas escolhas em vez de coagidas. Este é o cerne de que se trata a LGPD: a sociedade deve respeitar a liberdade individual, inclusive de suas escolhas econômicas. Este é o foco que norteará a ANPD. Da mesma forma, a Autoridade Nacional não pode tornar-se "vilã" das empresas, propiciando uma boa relação, sobretudo educacional para que disponhamos de padrões e técnicas que deem a verdadeira aplicabilidade e eficácia que se espera com a lei.

3.Quais empresas precisam se adequar a LGPD e quais dados são elencados

Conforme disposto na lei, todas as empresas que têm acesso a dados pessoais e/ou sensíveis devem se adequar à Lei Geral de Proteção de Dados, posto que, quem descumprir estará suscetível a advertências, sanções de até 50 milhões de reais ou até 2% do faturamento do ano anterior à multa.

O *compliance* das conformidades da lei precisa ser feito com uma avaliação de maturidade dos processos e impactos de riscos na empresa e redução dessa exposição ao risco, ou seja, avaliar todo o cenário empresarial e até onde esses dados são necessários para que os processos ocorram sem impacto. Em todos os outros casos, os dados deverão ser descartados se não forem disponibilizados e autorizados pelo detentor.

4.Quem pode tratar os dados das PME's?

Consoante a Lei Geral de Proteção de Dados Pessoais (LGPD), os principais sujeitos que podem tratar dados pessoais são:

> *Art. 5º Para os fins desta Lei, considera-se:*
>
> *VI - **controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;*
>
> *VII - **operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;*
>
> **IX - agentes de tratamento: o controlador e o operador; [GRIFO]**

O *Data Protection Officer* ou o Encarregado de Proteção de Dados (EPD) é o profissional responsável por auxiliar as empresas e administrações públicas para adequação às leis e de privacidade. Na GDRP, é exigido que as empresas nomeiem um DPO em algumas situações, quando por exemplo, se tratar de *Big Data* (grande quantidade dados pessoais) de

europeus, é necessário a nomeação de um DPO. No Brasil ainda não temos normativas definidas para dispensa ou necessidade de um DPO, entretanto, a LGPD em seu artigo 30 no inclina a esperar que esta orientação em breve será feita por legislação complementar pela ANPD:

> *Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.*

4.1 As certificações de institutos internacionais para profissionais no Brasil

Existem atualmente duas trilhas de certificações internacionais para o profissional de dados ser considerado DPO, sendo no Brasil mais comum a trilha da EXIN e, na Europa, da IAPP.

A trilha da EXIN implica a realização de três certificações distintas: a *Information Security Foundation (ISFS)*, a *Privacy and Data Protection Foundation (PDPF)* e, por fim, a *Privacy and Data Protection Practitioner (PDPP)*. No que se refere a *International Association of Privacy Professionals (IAPP),* os certificados oferecidos são: o *Certified Information Privacy Professional (CIPP), Certified Information Privacy Manager (CIPM) e Certified Information Privacy Technologist (CIPT).*

5.Como adequar as PME's a LGPD – Boas Práticas de Proteção de dados na Europa

A empresa especializada em segurança de informação "More It", em conjunto com a Associação Nacional de Profissionais de Privacidade de Dados – ANPPD, realizaram um Webinar[6] técnico em agosto de 2020, recomendando o modelo de boas práticas mais usado em todo mundo utilizando *o Privacy by designer,* framework construído pela canadense Ann Cavoukian, diretora executiva do Instituto de Privacidade e *Big Data* da Universidade de Ryerson, no Canadá.

5.1.1 *Privacy by Design*

A compreensão de *Privacy by Design*, ou "PbD", é uma concepção da Dra. Ann Cavoukian, diretora executiva do Instituto de Privacidade e *Big Data* da Universidade de Ryerson, no Canadá[7]. O *Privacy by Design* designa que todos os seus ciclos da metodologia de desenvolvimento de um produto ou serviço de uma entidade, devem obrigatoriamente ter a privacidade em primeiro lugar. Neste sentido, a compreensão de privacidade deve estar totalmente encastoada no projeto, e não se aplica a realizações onde a privacidade é discutida somente na fase final. O entendimento é que empresas que apliquem *Privacy by Design* nos projetos de desenvolvimentos de *software*, departamento de Tecnologia informação e

---

6 A Lei Geral de Proteção de dados em seu Artigo 32 e também em seu Capítulo VII, faz um recorte sobre as boas práticas que devem ser adotadas para adequação desta legislação, o conteúdo também foi explanado no Webinar da More IT em parceira com ANPPD (Associação Nacional dos Profissionais de Privacidade de Dados) trazendo esse treinamento de como adequar a LGPD e GDPR nas pequenas e médias empresas. O conteúdo ainda pode ser acessado pelo endereço: https://youtu.be/mYoD7S0mBGU

7 Conteúdo retirado do Webinar de treinamento da More IT em parceira com a ANPPD (Associação Nacional dos Profissionais de Privacidade de Dados) trazendo esse treinamento de como adequar a LGPD e GDPR nas pequenas e medias empresas aplicando *o Privacy By Designer. O* conteúdo ainda pode ser acessado pelo endereço: https://youtu.be/mYoD7S0mBGU

comunicação (TIC)e planejamentos estratégicos ataviados com a ideia de privacidade, e não como algo à parte.

5.1.2 *Privacy by Default*

A ideia de *Privacy by Default* (privacidade por padrão) significa que um produto ou serviço, ao ser emitido no negócio, deve vir com os formatos de privacidade no modo mais restrito possível por padrão, e o titular deve conceder acesso à colheita de mais informações caso considere necessário.

A maioria das grandes empresas de tecnologia fazem justamente o contrário, ou seja, coletam o máximo de informações possíveis por padrão, mas permitem que o titular desabilite a coleta de dados. Caso *Privacy by Default* fosse aplicado, os aplicativos coletariam somente o necessário e permitiriam que o titular habilitasse a coleta de dados extras, caso acredite que isso fosse algo benéfico.

5.1.3 – Os princípios do *Privacy by Design*

Vale ressaltar que o conceito de *Privacy by Design* estabelece sete princípios, que são:

5.1.3.1. Proativo, não reativo. Prevenir, não remediar.

O *PbD* reconhece o valor de agir proativamente para antecipar, identificar e prevenir invasões antes que elas ocorram. O melhor é não esperar que riscos de privacidade cheguem a se materializar, e sim evitar que eles aconteçam.

5.1.3.2. Privacidade por padrão.

O conceito de *Privacy by Design* também engloba o *Privacy by Default,* e isso permite que em um sistema que se guie por essas regras, mesmo que um usuário não faça nada, sua privacidade continue intacta. Dessa forma, não é necessário desativar a coleta de dados extras, já que ela deve vir desativada por padrão.

5.1.3.3 Privacidade embutida no design.

A privacidade deve ser algo totalmente embutida no design, arquitetura de T.I. e práticas corporativas. Não é algo adicional ou complementar, mas faz parte integral de toda a estrutura do produto ou serviço.

Sempre que possível, relatórios de prováveis impactos e riscos devem ser criados e publicados, claramente documentando os riscos de privacidade e todas as medidas tomadas para mitigá-los.

5.1.3.4. Total funcionalidade.

Ao implementar privacidade em um produto ou serviço, ela deve ser feita de forma a somar funcionalidades ao projeto, e não prejudicar nenhuma funcionalidade.

As funcionalidades que conflitem com princípios de privacidade devem ser modeladas de forma criativa para que possam funcionar juntos.

5.1.3.5 Segurança ponta a ponta.

A privacidade deve ser continuamente protegida através de todo o ciclo de vida dos dados em questão.

A segurança dos dados deve estar em mente desde o planejamento até a execução, implantação e manutenção do projeto.

5.1.3.6 Visibilidade e Transparência.

A coleta, processamento e armazenamento de dados devem ser documentados de forma totalmente transparente, incluindo informações sobre a responsabilidade dos dados em caso de algum vazamento ou invasão.

5.1.3.7 Respeito pela privacidade do usuário.

Deve ser sempre respeitada a decisão e a proteção dos dados do usuário, já que são propriedades dele. É necessário que haja consentimento no uso dos dados pessoais do usuário, com informações corretas e atualizadas conforme a necessidade. O usuário deve sempre ter acesso aos seus dados. É importante ressaltar que a LGPD não adotou os princípios de *Privacy by Design* ou *Privacy by Default* expressamente, mas traz alguns conceitos similares ao descrever medidas que as empresas devem tomar para proteção dos dados, ao estabelecer a necessidade de documentar a forma com que os dados pessoais são tratados e as medidas de proteção utilizadas.

Figura 01 – Ciclo de vida do Privacy by designer[8]

5.2 Ciclo de vida dos Dados na LGPD

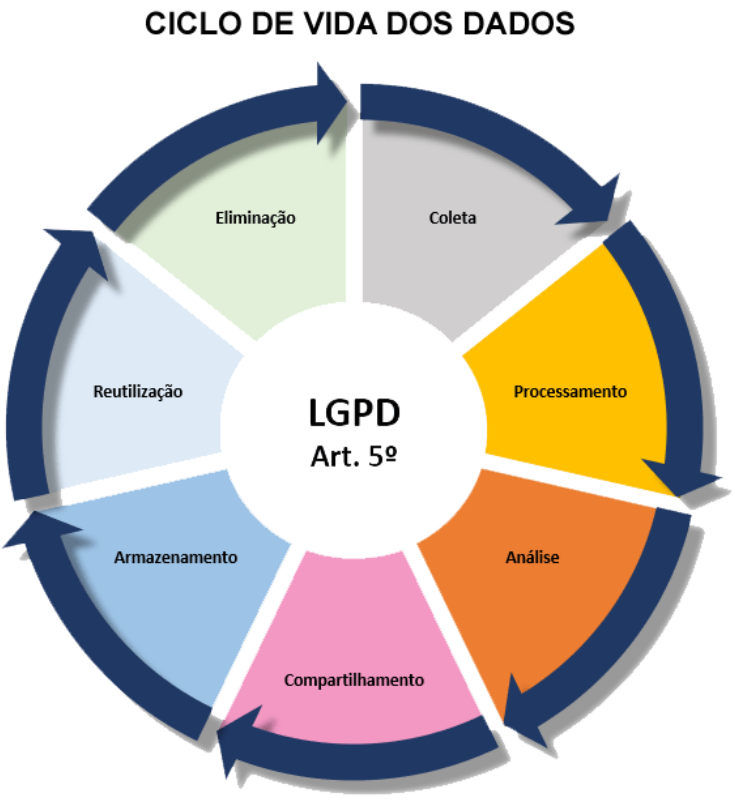
Considerando as boas práticas advindas da GDPR na Europa e também o artigo 5° da Lei Geral de proteção de Dados Incisos I, II, III:

Art. 5º Para os fins desta Lei, considera-se:

8 Figura do Ciclo de vida do *privacy by designer* e seus princípios apresentados no portal *Terms Feed* que pode ser acessado através do endereço: https://www.termsfeed.com/blog/privacy-design/

> *I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;*
>
> *II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;*
>
> *III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnico razoáveis e disponíveis na ocasião de seu tratamento;*
>
> *IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;*

Diante deste dispositivo e das boas práticas, entendemos da seguinte forma o ciclo de vida dos dados iniciando da coleta, conforme figura abaixo:



CICLO DE VIDA DOS DADOS		
FASE DO CICLO	**ANTES DA LGPD**	**COM A LGPD**
Coleta	Os dados pessoais são coletados indiscriminadamente.	Os dados pessoais coletados devem obedecer ao princípio da necessidade e da finalidade.
Processamento	Os dados podem ser processados sem um tratamento específico.	O processamento de dados só poderá ser realizado se o tratamento estiver enquadrado no Art. 7º da LGPD.
Análise	A análise de dados é feita para entender o mercado, conhecer o perfil das pessoas e definir estratégias para oferecer bens e serviços para o público-alvo.	A análise de dados deve levar em consideração a finalidade da coleta. Devem ser obedecidos os princípios de tratamento, com propósito legítimo, específico e explicito.
Compartilhamento	Os dados pessoais são compartilhados sem a necessidade do consentimento de seus titulares.	O compartilhamento de dados deve ser consentido pelos seus titulares.
Armazenamento	Os dados pessoais são armazenados e mantidos por tempo indeterminado.	Os dados pessoais devem ser armazenados e mantidos por prazos definidos, ou seja, até que finalidade seja alcançada ou deixem de ser necessários ou pertinentes ao alcance da finalidade.
Reutilização	Os dados pessoais são reutilizados sem a necessidade de consentimento de seus titulares.	Um novo consentimento deve ser solicitado sempre que houver mudança de finalidade.
Eliminação	Os dados pessoais são mantidos sem a obrigatoriedade de serem eliminados.	Os dados pessoais devem ser eliminados após o término de seu tratamento.

Figuras do Ciclo de vida dos dados analisados no contexto do artigo 5° da LGPD[9]

5.3 Principais diferenças e similitudes da GDPR com a LGDP

A privacidade e a proteção dos dados pessoais têm atingido cada vez mais espaço e magnitude no panorama mundial. A GDPR, lei europeia de proteção de dados, despertou pregressos para que no mundo inteiro os países prezem por fazer negócios valendo-se de dados pessoais concebidos por uma legislação que vise defender as pessoas. Isso faz que não haja nenhum excesso de dados, como houve no alvoroço da *Cambridge Analytica* em relação ao Facebook.

Não obstante, já que cada nação ou conglomerado de estados têm sua própria legislação, é corrente que estejamos hesitantes.

A LGPD e a GDPR são regulamentos de privacidade de dados e, como todo regulamento, seu texto é longo e detalhado. Mas, para facilitar o entendimento, elencamos as principais semelhanças e diferenças. São seis diferenças principais:

a) Território em que cada um é válido:

A LGPD será válida em todo o território brasileiro.

A GPDR é válida em toda a União Europeia.

b) Há quais titulares de dados se aplica a lei:

9 Escopo e desenho coletado do portal XPOSITUM que pode ser visto em https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd

A LGDP se aplica a titulares naturais, ou seja, dados pessoais de pessoas físicas.

A GDPR é aplicável aos dados pessoais dos titulares dos dados, ou seja, os usuários. Podem ser clientes ou meros visitantes de um site.

c) A definição de dado pessoal:

Para a LGPD, dado pessoal é toda informação relacionada a uma pessoa identificada ou identificável. Existem informações que não te identificam pessoalmente, portanto você continua anônimo. Há outras, no entanto, que te identificam individualmente, como nome, e-mail e documentos pessoais.

Para a GDPR, tudo isso é dado pessoal. E há ainda duas categorias distintas: dados tornados públicos pelo próprio titular e dados relacionados a instituições sem fins lucrativos. Entre essas definições, de dados pessoais, anônimos ou não, há uma mais especial: dados sensíveis. A GDPR, ao contrário da LGPD, proíbe o uso de dados sensíveis, a não ser que esse uso esteja previsto em lei.

d) Quem trata os dados:

A LGPD e a GDPR, em seus respectivos territórios, se aplicam a todo tratamento de dados, com exceção do uso particular. Se é uma empresa, uma ONG ou uma instituição do governo, pouco importa: a lei se aplica.

e) Venda de dados pessoais:

Na LGPD e na GDPR, para que a venda de dados pessoais seja feita, é necessária uma base legal prevista na lei, não podendo ser realizado o serviço por qualquer pessoa.

f) Multas e penalidades

A GDPR e a LGPD e empregam multas e penas diferentes, por conseguinte, cada uma deve ser folheada em particular, avaliando, inclusive, o caso concreto.

g) Transparência sobre o uso de dados:

Os dois regulamentos preservam transparência conforme ao uso de dados: se estão sendo tratados, se podem ser vendidos e com que destino estas atividades são praticadas.

h) Faculdade de atualizar e eliminar dados

Os dois regulamentos consentem que os usuários revoguem a concessão dos dados, bem como abonam que ele consiga atualizá-los quando bem entender.

i) Autoridade responsável

Os regulamentos constituem uma autoridade oficial para salvaguardar que a lei seja efetivada. No caso da LGPD, é a Autoridade Nacional de Proteção de Dados.

5.4 Documentos que devem ser criados como boas práticas de adequação a proteção da privacidade de dados:

Ressaltamos aqui, que embora citaremos alguns documentos que não são obrigatórios na LGPD[10], é uma boa prática construí-los, uma vez que tratando dados de estrangeiros que têm em seu país legislação de proteção de dados, em especial os da União Europeia, mesmo que os dados sejam tratados no Brasil, estes pertence a pessoa natural de outro país, portanto devendo ser considerado a legislação extraterritorial, em especial a GDPR.

a) Documentos mandatários na LGPD:

- ✓ Política de proteção de dados
- ✓ Aviso de privacidade
- ✓ Aviso de privacidade para funcionários
- ✓ Política de retenção de dados
- ✓ Cronograma de retenção de dados
- ✓ Formulário de consentimento do titular
- ✓ Formulário de consentimento dos pais
- ✓ Nomeação e descrição de cargo DPO

b) Documentos criados para atender as boas práticas da GDPR para aplicação <u>não</u> mandatárias na LGPD:

- ✓ Registro de inventário;
- ✓ Nomeação do DPO;
- ✓ Registros de AIPD (AIPD – Avaliação de Impacto na Proteção de Dados);
- ✓ Contrato de Processamento de dados do fornecedor;
- ✓ Procedimento de resposta e notificação de violação de dados;
- ✓ Registro de violação de dados;
- ✓ Formulário de notificação da violação de dados para autoridade supervisora.

6.Consequências jurídicas da não adequação da LGPD das PMEs

As consequências jurídicas para as PME's que não se adequarem à LGPD podem ser de multa de até 2% em cima do faturamento anual ou, no máximo, em R$50 milhões por infração. Mas há outras questões que, mesmo não sendo tão debatidas, podem influenciar nos negócios e prejudicar a empresa como um todo, como os problemas comerciais, visto que uma empresa que não cumpre a lei pode ter empecilhos com parceiros e clientes próximos. Isso acontece

10 Orientações feitas pelo PhD Davis Alves, presidente da Associação Nacional dos Profissionais de Privacidade de Dados no Webinar da More IT que pode ser visto no endereço: https://youtu.be/mYoD7S0mBGU

porque o consumidor final dos produtos e/ou serviços está cada vez mais criterioso, desconfiando de corporações que não contam com boas práticas internas.

O impacto com contatos internacionais será ainda mais severo, uma vez que, muitos países já estão em dia com o plano de proteção de dados. Podemos elencar também os riscos financeiros que, como observado na própria legislação, se tratam de uma penalidade mais grave para as empresas, que é a sansão aplicada de acordo com a violação ao que é previsto por lei. Entretanto, mesmo arcando com as sanções, não se adequar à LGPD pode trazer outros riscos financeiros, uma vez que pode impactar negativamente em todos os setores. Na perspectiva da governança, uma organização que não tem critérios de *compliance* pode vir a acabar com sua imagem e até mesmo falir.

Como dito em linhas volvidas, a penalidade com valores como os praticados na LGPD, que a princípio parecem exorbitantes e impraticáveis, já é uma realidade na Europa com a GDPR, onde ocorreu o caso da empresa Google, que foi multada pela CNIL por cinquenta milhões de euros por uso de dados pessoais. As consequências jurídicas da não adequação à LGPD estão expostas no Capítulo VIII, da fiscalização, Seção I – Das sanções administrativas. Dentre elas, destaca-se que, além das peculiaridades do caso concreto, deverá ser considerado também a boa-fé do infrator, a reincidência, a vantagem auferida ou pretendida e a cooperação do infrator. Entretanto, na base mesma desses argumentos, e por vezes se opondo a eles, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, a adoção de política de boas práticas e governança e a pronta adoção de medidas corretivas transmitem não só à Autoridade Nacional, mas também aos consumidores, que a empresa pretende proporcionar o máximo de segurança em seus produtos e/ou serviços.

Destaca-se que, da mesma forma que a ANPD observa as peculiaridades de cada caso, o processo de *compliance* à LGPD também deverá ser personalizado para cada empresa, não sendo possível uma receita genérica para todos os segmentos. Caberá as empresas aproveitarem dessa lacuna abstrata que a lei proporciona em seu início para buscarem na doutrina e na jurisprudência – que também estão, de certa maneira, em fase educacional acerca do tema – conceitos que se acomoda melhor ao mercado consumerista e econômico.

7.Potencial aumento de demandas judiciais envolvendo titulares e operadores de dados:

A entrada em vigor da LGPD traz consigo algo que até então não era muito observado pelo senso comum, que é a importância de protegerem os seus dados pessoais, tendo em vista os riscos que a coleta, compartilhamento, tratamento e rastreio comportamental podem acarretar na vida de jovens, adultos, idosos e até mesmo crianças que já fazem uso de aparelhos eletrônicos. Outrossim, a conscientização das pessoas acerca do tema pode desenfrear uma disputa judiciária maçante, assim como já ocorre em outras searas consumeristas.

Nesse sentido, caberá às pequenas e médias empresas, que são maioria no país e não possuem grande capital para lidar com demandas que, em sua maioria, pretendem condenação em danos morais, pensar de forma estratégica para criar alternativas junto aos atores envolvidos – SENACON, Instituto Brasileiro de Defesa do Consumidor, Ministérios Públicos Federal e Estaduais, associações de defesa do consumidor, associações que tratem especificamente de proteção de dados, bem como a ANPD – possibilitando uma renovação nas políticas de defesa do consumidor sem que haja congestionamento judicial.

Soma-se a isso a necessidade de implementação de resolução de conflitos não só com sanções, mas também com atividades educacionais, acessíveis e gratuitas, experimentando métodos extrajudiciais e administrativos, como a conciliação e mediação.

É interessante que os meios alternativos de solução de controvérsias sobre proteção de dados proporcionem não só o ressarcimento do consumidor ofendido, mas também sugestões de modificação dos procedimentos internos da empresa para que não se torne reincidente, evitando por exemplo a aplicação do artigo 52, V da LGPD. Ressalta-se que o intuito não é ferir o princípio da inafastabilidade da jurisdição, previsto no artigo 5º, inciso XXXV da Constituição Federal, prevendo a necessidade de exaurimento de procedimento administrativo para que se reconheça o direito previsto em lei, apenas evitar o congestionamento do judiciário e dar ao consumidor uma resposta célere e amigável que não precisa ser imposta por sentença judicial.

De modo geral, esses mecanismos alternativos são estabelecidos por órgãos regulatórios, como a ANPD, em parceria com o poder judiciário, seguindo os princípios do contraditório e ampla defesa para possibilitar a negociação, mas figurando como fiscalizador de casos repetitivos e não necessariamente exercendo a função de resolução de conflitos.

E, partindo dessa premissa e tendo em vista que a lei é abarcada pela inovação do Direito Virtual e não exclui ou condiciona o acesso à justiça, mas estimula a autocomposição, devemos ter a tecnologia como meio prático para evitar o excesso de judicialização, implementando meios consensuais céleres e acessíveis. Temos como exemplo prático, inclusive, a plataforma consumidor.gov.br, formalizada através do Decreto nº 8.573/2015 e alterada pelo Decreto nº 10.197/2020, que é uma ferramenta pública gratuita, que permite a interlocução direta entre consumidores e empresas para solução de conflitos de consumo pela internet, monitorada pela SENACON, Ministérios Públicos e da Justiça, Procons e Defensorias.

Haverá necessidade de se oferecer respostas rápidas e eficazes aos titulares de dados pessoais, colocando em evidência no mercado as empresas que preocupam-se em evitar os danos e/ou repará-los com agilidade, bem como os profissionais que atuam nas áreas do Direito e Tecnologia da Informação que buscam ideias inovadoras tal qual a lei criada.

8.O que as PME's devem fazer em caso de vazamento de dados

No campo teórico, o artigo 46 da LGPD dispõe que é dever dos agentes de tratamento – ou qualquer outra pessoa que intervenha em uma das fases do tratamento – a adoção de 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.

Pensando nisso, é recomendado que haja restrições de acesso, treinamento de funcionários, boa infraestrutura de Tecnologia da Informação, backups periódicos, dados criptografados, sistemas de softwares confiáveis desde a fase de concepção do produto ou do serviço até a sua execução, bem como um Plano de Recuperação de Desastres (DRP — *Disaster Recovery Plan*).

Ademais, a ANPD precisa ser comunicada sobre o vazamento, conforme determina o Capítulo VII da LGDP que trata da Segurança e das boas práticas e, mais que isso, embora não seja uma exigência, mas à autoridade poderá dispor sobre padrões técnicos mínimos para tornar aplicáveis as medidas de segurança, considerados a natureza das informações tratadas, as

características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis.

Embora a empresa esteja dentro dos padrões estabelecidos em lei, é importante saber lidar com possíveis incidentes, tendo em vista que os crimes virtuais vivem uma crescente devido a ampliação do mercado econômico digital.

Para que se mantenha um bom relacionamento com a ANPD e com os consumidores, o controlador deverá comunicar à Autoridade Nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. A lei, contudo, em seu §1º do artigo 48 não indica qual o prazo razoável para que seja feita a comunicação, deixando a sua definição a cargo da Autoridade Nacional. Entretanto, sabe-se que a comunicação deverá mencionar, no mínimo: a descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança utilizada para a proteção dos dados, observados os segredos comercial e industrial; os riscos relacionados ao incidente; os motivos da demora, no caso de a comunicação não ter sido imediata e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

É competência da Autoridade Nacional verificar a gravidade do incidente e tomar medidas para salvaguardar os direitos dos titulares, bem como buscar a reversão e mitigação dos prejuízos. Outrossim, também ficará incumbida de avaliar eventuais medidas técnicas tomadas pela empresa, bem como os sistemas e estruturas utilizadas para o tratamento dos dados. Por isso nunca é demais ressaltar a importância de atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na lei e às demais normas regulamentares, conforme disposto no artigo 49 da LGPD.

Alinhados as essas diretrizes, o controlador e/ou operador que for considerado responsável pelo dano patrimonial, moral, individual ou coletivo após procedimento administrativo pautado nos princípios do contraditório e ampla defesa deverá ser obrigado a repará-lo nos parâmetros e critérios elencados no artigo 52 da LGPD. Portanto, é importante que se demonstre boa-fé, coopere com as autoridades competentes, adote políticas de boas práticas e governança, bem como mecanismos capazes de minimizar ou reparar os danos.

Por fim, além de se preocuparem com a responsabilidade solidária e o direito de regresso no ressarcimento dos danos, os agentes de tratamento devem se ater as exceções trazidas no artigo 43 da lei.

> *Art. 43. 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 terceiro.*

Por conseguinte, está cada vez mais importante a introdução de profissionais capacitados no ramo da Tecnologia da Informação e Direito Digital para resguardar a empresa e deixá-la em evidência não só à Autoridade Nacional, mas também aos consumidores e parceiros multinacionais que já estão mais avançados na adaptação imposta pela GDPR.

9.Conclusão

A Lei Geral de Proteção de dados LGPD vai trazer profundas transformações em matéria de proteção dos dados pessoais no Brasil, acarretando impactos para inúmeras empresas – de pequeno ou grande porte – e também para outras instituições, inclusive para a Administração Pública. Apesar da ampla vacância estabelecida – originalmente, de dezoito meses, depois na tentativa fracassada de postergar sua vacância pelo Governo do presidente Jair Messias Bolsonaro, através da MP959/2020 que tentou estender o prazo para maio de 2021 para as vigências e agosto de 2021 para o início das aplicações de penalidades. O governo negociou inicialmente com o congresso uma data que atendia ambos os interesses: 31 de setembro de 2020. O cenário de crise política, econômica e sanitária que se ilustra o estado brasileiro, fez com que o Senado desfizesse o acordo com o governo, deixando a MP 959/2020 caducar, ou seja, não sendo convertida em lei, logo sua eficácia iniciou nos 15 dias uteis subsequentes, no caso, dia 18 de setembro de 2020, tento sido no mês posterior feito as nomeações para composição e regulamentação da ANPD para execução da LGPD já em 2020 e bem antes do acordado anteriormente entre governo e congresso.

Nessa direção de aplicação da LGDP já em 2020, levanta vários questionamentos sobre a adequação tanto do mercado quanto da administração pública a legislação aprovada em 2018. Outro ponto que chama atenção, é sobre a Autoridade Nacional de Proteção de Dados – ANPD, que foi composta por indicações do presidente Jair Messias Bolsonaro por cinco nomes, três deles, militares ligados à sua família, o que coloca em discussão a autonomia e parcialidade da ANPD.

Nesse contexto, baseamos este artigo nos modelos já utilizados na Europa com a GDPR e no que vem sendo considerado boas práticas de segurança da informação e de proteção de dados em todo mundo, como o *framework Design by privacy.*

Por fim, torna-se absolutamente relevante que as pequenas e médias empresas, assim como a administração pública, devem se adequar à nova legislação, não apenas para evitar penalidades, mas também para garantia da proteção dos dados pessoais, hoje com status de direitos fundamentais pelo ONU, promovendo maior segurança jurídica, proteção dos direitos dos titulares e correlação de forças no mercado.

10.Referência bibliográfica

BRASIL. Lei complementar n° 123, de 14 de dezembro de 2006. **Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm >. Acesso em: 10 de maio de 2020

BRASIL. Lei N°13.709 de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >. Acesso em: 10 de maio de 2020

ANPPD – Associação Nacional de Profissionais de Proteção de Dados. **Pareceres Técnicos**. Disponível em: < https://anppd.org/pareceres-tecnicos > Acesso em: 10 de maio de 2020

CFA – Conselho Federal de Administração. **Ancoras da Economia**. Disponível em: < http://www.cfa.org.br/ancoras-daeconomia > Acesso em 10 de maio de 2020.

PRIVACY virtuoso. ***Privacy By Design***. Disponível em: < https://privacyvirtuoso.com/privacy-design.php > Acesso em 10 de abril de 2020.

MORE IT. **LGPD - Como as PMEs devem enxergar a adequação?**. Disponível em: < https://www.youtube.com/watch?v=mYoD7S0mBGU > Acesso em 16 de abril de 2020.

CONJUR, Consultor Jurídico. **Postergação da vigência da LGPD: um remédio necessário?** Disponível em < https://www.conjur.com.br/2020-mai-01/direito-civil-atual-postergacao-vigencia-lei-geral-protecao-dados-remedio-necessario > Acesso em 20 de junho de 2020.

CÂMARA dos deputados. **Medidas Provisórias – Relatoria, obstrução e prazo final.** Disponível em < https://www.camara.leg.br/internet/lideres/MedidasProvisorias.pdf > Acesso em 20 de junho de 2020.

SEBRAE. **Micro e pequenas empresas geram 27% do PIB do Brasil.** Disponível em <https://www.sebrae.com.br/sites/PortalSebrae/ufs/mt/noticias/micro-e-pequenas-empresas-geram-27-do-pib-do-brasil,ad0fc70646467410VgnVCM2000003c74010aRCRD> Acesso em 10 de abril de 2020.

CNIL. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC**. Disponível em: < https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc > Acesso em 20/06/2020.

FOLHA. **França multa Google em 50 milhões de euros por uso de dados pessoais**. Disponível em < https://www1.folha.uol.com.br/mercado/2019/01/franca-multa-google-em-50-milhoes-de-euros-por-uso-de-dados-pessoais.shtml > Acesso em 20/06/2020.

CONGRESSO de proteção de dados. **Os princípios do Privacy by designer**. Disponível em:<https://www.congressodeprotecaodedados.com.br/2019/ppt2019/2.1_PPT_WKS_%20PRIVACY%20AND%20SECUTIRY.pdf > Acesso em 20/06/2020.

BRASIL, Decreto nº 10.474**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm> Acesso em 20/10/2020.

CALIFORNIA Legislative Information. **California Consumer Privacy Act**. Disponível em <http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 > Acesso em 20/10/2020.

INTERSOFT Consulting. **General Data Protection Regulation GDPR**. Disponível em: < https://gdpr-info.eu/ > Acesso em 20/10/2020.

TERMS Feeds. **Privacy by Design**. Disponível em: < https://www.termsfeed.com/blog/privacy-design/ > Acesso em 01/11/2020.

BRASIL, Congresso. **Inteiro teor PEC 17 Proposta de Emenda à Constituição**. Disponível em:< https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757 > Acesso em 01/11/2020.

XPOSITIUM. **Ciclo de Vida dos Dados e LGPD**. Disponível em: < https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd > Acesso em 01/11/2020.