Organizadoras:
Amanda Maíra Rodrigues dos Santos
Poliane Almeida Silva Dias

Autoras:
Amanda Maíra Rodrigues dos Santos
Jéssica Lorena da Silva Pinheiro
Pauliana Roberta Mota de Abreu
Poliane Almeida Silva Dias

LGPD PRÁTICA
PARA MICRO E PEQUENAS EMPRESAS

Prefácio: Rafael Susskind

EXPERT
EDITORA DIGITAL

OAB MINAS GERAIS
82ª Subseção
Betim

O Livro LGPD Prática - Para Micro e Pequenas Empresas escrito pelos Membros da Comissão de Proteção de Dados da OAB/MG Subseção Betim, aborda questões essenciais para Micro e Pequenas Empresas (MPEs), com foco na importância da comunicação e na conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

O Livro destaca de forma prática como os empreendedores no Brasil poderão iniciar medidas técnicas e organizacionais para proteger os dados pessoais, garantir a transparência e possibilitar que os titulares dos dados exerçam seus direitos frente a LGPD.

Enfatizando a importância da comunicação para o crescimento das MPEs, destacando que muitas não estão preparadas para comunicar seus negócios de maneira eficaz. Trazemos ainda o Registro Simplificado de Operações de Tratamento de Dados Pessoais (ROPA) como uma ferramenta essencial para a conformidade com a LGPD, um modelo em Legal Design irá facilitar o entendimento sobre o tema.

Também abordamos como as MPEs podem se proteger contra incidentes de segurança e agir em caso de ocorrência. Mesmo com medidas de proteção, novos desafios cibernéticos surgem constantemente, exigindo que as empresas estejam preparadas para mitigar riscos e comunicar incidentes à Autoridade

No geral, o Livro oferece uma análise detalhada e prática de como as MPEs podem se adaptar à LGPD, enfatizando a importância da comunicação eficaz e da adoção de medidas de proteção de dados. A conformidade com a LGPD é viável com investimento adequado e pode ser alcançada por empresas de qualquer porte.

ISBN 978-65-6006-090-6

OAB MINAS GERAIS
82ª Subseção Betim
EXPERT EDITORA DIGITAL

LGPD PRÁTICA
PARA MICRO E PEQUENAS EMPRESAS

Direção Executiva: Luciana de Castro Bastos
Direção Editorial: Daniel Carvalho
Diagramação e Capa: Editora Expert
A regra ortográfica usada foi prerrogativa do autor

Dados Internacionais de Catalogação na Publicação (CIP)

SANTOS, Amanda Maíra Rodrigues dos;
DIAS, Poliane Almeida Silva
Titulo: LGPD Prática - Para Micro e Pequenas Empresas - Belo Horizonte - Editora Expert - 2024
Organizadores: Amanda Maíra Rodrigues dos Santos
Poliane Almeida Silva Dias
ISBN: 978-65-6006-090-6
Modo de acesso: https://experteditora.com.br
1.Direito Empresarial
2.Lei Geral de Proteção de dados
3.Micro e pequenas empresas
4.Comunicação I. I. Título.
CDD: 342.2

Pedidos dessa obra:

experteditora.com.br
contato@editoraexpert.com.br

82ª Subseção
Betim

MINAS GERAIS

Comissão de
Proteção de Dados

Livro: *LGPD Prática - Para Micro e Pequenas Empresas*

Organizadoras:
Amanda Maíra Rodrigues dos Santos
Poliane Almeida Silva Dias

Autoras:
Amanda Maíra Rodrigues dos Santos
Jéssica Lorena da Silva Pinheiro
Poliane Almeida Silva Dias
Pauliana Roberta Mota de Abreu

PREFÁCIO

É amplamente conhecida a dificuldade de empreender no Brasil, devido à complexidade legislativa, a burocracia excessiva, a elevada carga tributária e a constante instabilidade econômica. Estes são desafios diários para as micros e pequenos empresários do país. Em 2020, a Lei Geral de Proteção de Dados Pessoais (LGPD) foi adicionada ao rol de obrigações a serem seguidas por essas empresas.

A LGPD, em resumo, exige que as empresas adotem medidas técnicas e organizacionais para assegurar a proteção dos dados pessoais que tenham em seu poder. Além disso, determina que as empresas adequem seus processos para tratar estes dados pessoais apenas para finalidades legítimas, específicas e utilizando apenas os dados estritamente necessários, garantindo ainda transparência ao titular e possibilidade de ele exercer seus direitos estabelecidos na legislação.

Tendo atuado em projetos de adequação à LGPD e como DPO (Data Protection Officer ou Encarregado de Dados) para diversas empresas, posso afirmar que atingir a conformidade com a legislação é possível para qualquer empresa, com um investimento relativamente baixo.

Muitos empreendedores já adotam medidas mínimas de segurança dos dados, conscientes de que ataques cibernéticos podem causar grandes prejuízos financeiros e degradar a imagem da empresa perante clientes, parceiros e investidores. Qualquer empresário, independente do porte e segmento em que atua, sabe que os valores gastos nesta área são cruciais para garantir a continuidade dos negócios.

Importante ressaltar que a LGPD não estipula um investimento específico em segurança ou a obtenção de certificações reconhecidas, mas requer que as empresas adotem medidas consideradas adequadas ao seu porte e segmento. Portanto, não se espera que pequenas empresas disponham da mesma estrutura de segurança que as grandes corporações.

No que diz respeito às medidas organizacionais, cada empresa deve revisar e ajustar seus processos, estabelecendo políticas e procedimentos que garantam que os dados pessoais sejam tratados conforme a legislação exige.

A Autoridade Nacional de Proteção de Dados (ANPD) instituiu um regulamento especial para micro e pequenas empresas, facilitando algumas exigências e, consequentemente, diminuindo os custos e o tempo para o projeto de adequação à LGPD. No entanto, apesar dessas simplificações, o regulamento não dispensa essas empresas de cumprirem os requisitos fundamentais previstos na lei.

A LGPD também aborda a governança, exigindo que todas as medidas sejam regularmente revisadas e aprimoradas para garantir a continuidade do projeto. Privacidade e proteção de dados devem ser incorporadas à cultura da empresa.

Todas as providências detalhadas acima são um resumo dos procedimentos necessários para estar em conformidade com a legislação. É inegável que o projeto demanda tempo, esforço e investimento, porém, não em uma magnitude que inviabilize o projeto.

Muitos empreendedores questionam a efetividade da LGPD, considerando que até o momento poucas empresas foram sancionadas pela ANPD e acreditam que apenas grandes empresas deveriam estar sujeitas a este tipo de regulamento.

Quatro anos após o início da vigência da lei, minha experiência comprova a importância da adequação pelas pequenas empresas. Não pelo temor de multas e sanções, mas para a obtenção de um diferencial competitivo e a valorização da marca, especialmente para empresas B2B que prestam serviços a empresas maiores.

Um dos aspectos mais importantes da LGPD é o seu efeito cascata. A empresa que controla os dados pessoais deve garantir que todos os terceiros com quem compartilha esses dados também estejam em conformidade com a legislação e adotem medidas técnicas e organizacionais para proteger esses dados. Assim, grandes empresas devem realizar uma due diligence em seus parceiros e prestadores de serviço para confirmar essa adoção.

Muitas empresas de pequeno porte nos procuram depois de receberem de um cliente um questionário que solicita evidências das medidas de conformidade adotadas. Situação semelhante ocorre durante processos de fusões, aquisições e captação de investimentos, nos quais os investidores buscam confirmar se estão aplicando recursos em uma empresa que cumpre com as leis e normativas aplicáveis.

Estar em conformidade com a LGPD é um diferencial competitivo e demonstra para clientes, parceiros, fornecedores e colaboradores a seriedade e profissionalismo da empresa. Estes são fatores importantes que levam à consequente valorização da marca.

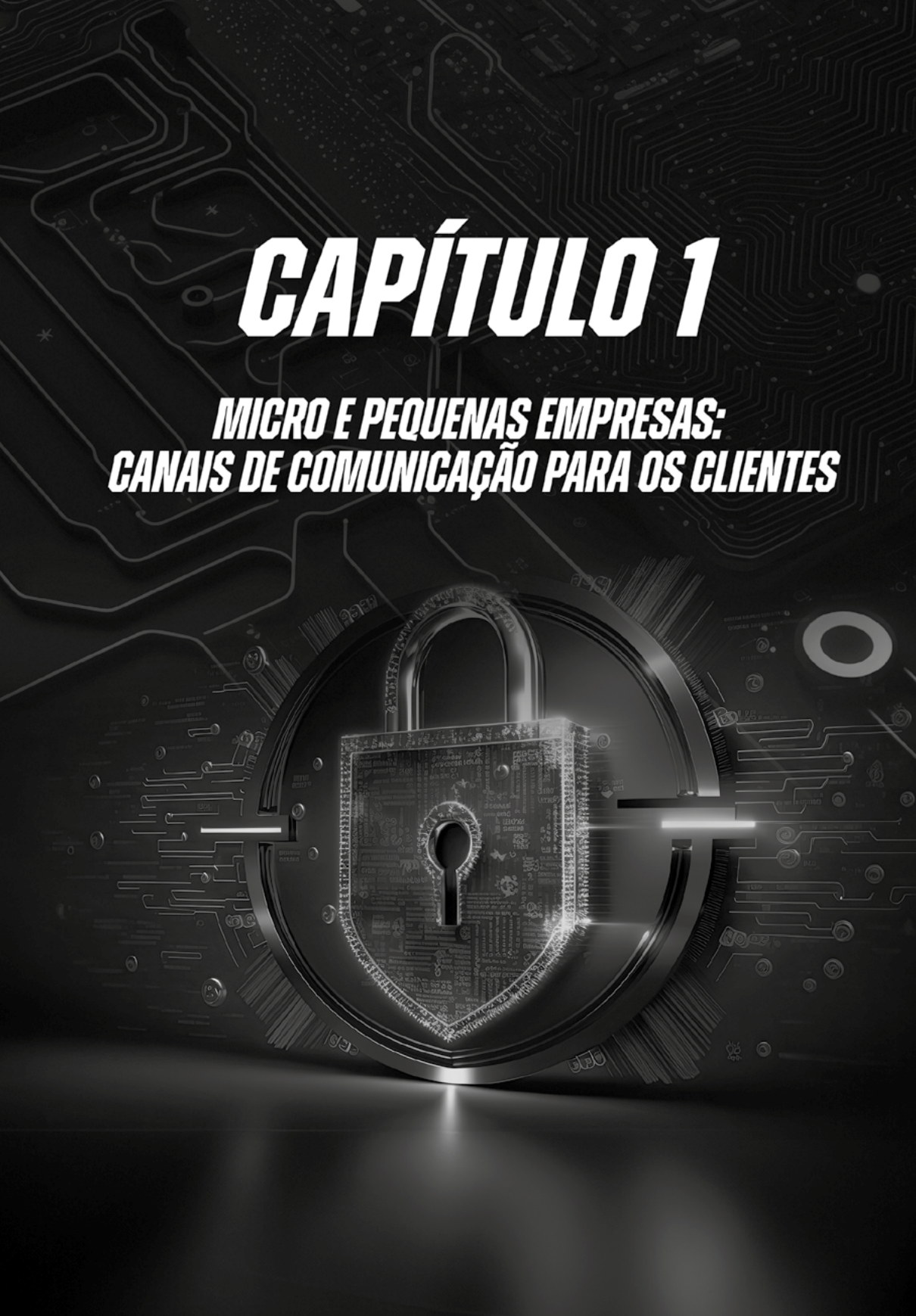
Esta obra oferece diretrizes práticas para auxiliar o empreendedor em seu projeto de adequação, abordando as particularidades e especificidades da legislação para microempresas e empresas de pequeno porte. Apesar de conciso, este livro contém dicas valiosas que servirão de guia para ajudar estas empresas em sua jornada de conformidade com a LGPD.

Rafael Susskind
Sócio-fundador da DPO Expert, tendo atuado em mais de uma centena de projetos de adequação; DPO as a Service de dezenas de empresas; IAPP Certified Information Privacy Manager (CIPM); IAPP Certified Data Protection Officer (CDPO); Exin Data Protection Officer; Analista de Cybersecurity pelo Inst. de Gestão e Tecnologia da Informação. @dpoexpert

SUMÁRIO

CAPÍTULO 1

MICRO E PEQUENAS EMPRESAS: CANAIS DE COMUNICAÇÃO PARA OS CLIENTES



Amanda Maíra Rodrigues dos Santos[1]

RESUMO: As micro e Pequenas Empresas (MPE) representam toda a realização do empreendedorismo, visto que o empreendedorismo é a melhor saída para o desenvolvimento social, educacional e sustentável de qualquer país. Por isso, como parte do desenvolvimento das micro e pequenos negócios, a comunicação é o grande passo para o crescimento, mas infelizmente as micro e pequenas empresas não estão preparadas para fazer a comunicação dos seus negócios, e poucas sabem ou reconhecem a sua importância como a principal ferramenta para inserir uma marca, um produto, um negócio ou até mesmo um segmento no mercado. Nesse contexto, o surgimento da Lei Geral de Proteção de Dados Pessoais (LGPD) [2] trouxe consigo a aplicação de regulamentos a instituições públicas e privadas que processam informações pessoais para que se adaptem à referida Lei. Este estudo se concentra em apontar os desafios e impactos enfrentados pela sociedade em consonância ao cumprimento da LGPD. A metodologia aplicada trata-se da pesquisa bibliográfica qualitativa-descritiva. Portanto, por meio do estudo, observa-se a complexidade e a importância em criar uma cultura organizacional e diretrizes para uma boa e apropriada governança e conduta de boas práticas relacionadas ao tratamento de dados pessoais na sociedade atual.

PALAVRAS-CHAVE: Microempresa - Canais de comunicação - Lei Geral de Proteção de Dados Pessoais –Sociedade - Sistema informacional.

---

1 Amanda Maíra Rodrigues dos Santos: Advogada, Mestre em Direito Privado pela FUMEC, Pós-graduada em Direito do Trabalho, Direito Civil e Direito Previdenciário ambos pela IPEMIG, Palestrante, Professora de Direito, pesquisadora de Direito e Tecnologia pela UFMG, Vice- Presidente da Comissão de Proteção de Dados da OAB/MG Subseção de Betim. @amandaadvogada

2 BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/l13709.htm . Acesso em: 14 abr. 2024.

ABSTRACT: Micro and Small Enterprises (MSEs) represent the entire realization of entrepreneurship, since entrepreneurship is the best way out for the social, educational and sustainable development of any country. Therefore, as part of the development of micro and small businesses, communication is the great step for growth, but unfortunately micro and small companies are not prepared to communicate their business and few know or recognize its importance as the main tool to insert a brand, a product, a business or even a segment in the market. In this context, the emergence of the General Personal Data Protection Law (LGPD) [3] brought with it the application of regulations to public and private institutions, which process personal information, if they comply with said Law. This study focuses on pointing out the challenges and impacts faced by society in line with compliance with the LGPD. The methodology applied in this research is the qualitative-descriptive bibliographic research. Therefore, through the study, it is observed the complexity and importance of creating an organizational culture and guidelines for a good and appropriate governance and conduct of good practices related to the processing of personal data in today's society.

KEYWORDS: Micro Enterprise - Communication channels - General Personal Data Protection Law – Society - Information system.

1. INTRODUÇÃO

Segundo Amyx (2009), um dos maiores desafios significativos é a percepção negativa em relação às Micros e Pequenas Empresas - MPE. Os clientes potenciais percebem as pequenas empresas por falta de capacidade em fornecer serviços de qualidade e são incapazes de satisfazer mais de um projeto crítico simultaneamente. Muitas vezes, empresas maiores são selecionadas entre negócios por sua influência na indústria e reconhecimento de nome.

3 BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/l13709.htm . Acesso em: 14 abr. 2024.

Começar e operar uma pequena empresa inclui a possibilidade de sucesso, bem como falha. Por causa de seu tamanho, um simples erro de gerenciamento provavelmente levará à queda de uma pequena empresa, portanto, existe a oportunidade de aprender com seus erros do passado.

A dinâmica e o crescimento das economias dos países em desenvolvimento, conhecido como país emergente, depende muito da ocupação da empresa. Essas empresas de porte pequeno podem sobreviver de forma sustentável e gerar empregos e renda para as pessoas. Portanto, é de elevada importância orientar esses países a alcançarem níveis mais elevados de produção de bens e serviços, e posicionamento estratégico na economia interna e externa (FERREIRA et al., 2013).

O número de PMEs no Brasil continua crescendo segundo a consultoria Empesômetro, cerca de 70% dos 20 milhões de empresas brasileiras se enquadram nessa categoria. Segundo o Serviço de Apoio à Micro e Pequena Empresa do Brasil (SEBRAE), em fevereiro de 2019, eles geravam 72% dos empregos oficiais do País, o maior saldo do mês em relação aos dois anos anteriores.

Segundo o Portal Brasil (2014), em 2010, 58% das pequenas empresas foram fechadas antes de completar cinco anos. Comparado com 2009, o índice é 62%. Um dos principais motivos descritos pelos empresários é a falta de clientes (29%), capital (21%), competição (5%), burocracia e tributação (7%).

Os avanços na tecnologia trouxeram um aumento na velocidade das atividades cotidianas. Um exemplo é o processo de comunicação, que é nos últimos 20 anos, começando com cartas que levaram dias, às vezes semanas ou até meses para entregar as mensagens instantâneas que hoje o telefone faz em questão de segundos. Por trás de todas essas evoluções, está o fato de que as informações foram adquiridas por meio de um novo patamar de importância, especialmente para as empresas em formação que precisam estar no lugar certo, na hora certa, com as pessoas certas. A velocidade e qualidade da informação tornou-se uma vantagem competitiva para as organizações.

Nos últimos anos, o número de usuários com acesso à Internet e o número de informação disponível aumentou significativamente. Este aumento está relacionado com a liberdade de dados fornecidos pela rede. Com o desenvolvimento de novas tecnologias, a comunicação contínua entre dispositivos e pessoas facilita a troca de informações, criando maior valor de dados que são armazenados e processados por questões de segurança da informação são coletadas (RAPOSÔ, 2019).

A Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais -LGPD, que entrou em vigência a partir de 18 de setembro de 2020, adotou sanções administrativas somente a partir de 1º de agosto de 2021. Consequentemente, pelo seu valor, qualquer pessoa física ou jurídica rege-se pelo direito público ou o particular que processa os dados pessoais que cumpre instruções fornecidas por regulamentos legais. E isso permite dizer que, os dados das pessoas naturais que estiverem sob custódia desses agentes de tratamento, deverão estar protegidos por meio da utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Diante do exposto, o presente estudo tem por objetivo determinar os desafios enfrentados pelas micro e pequenas empresas brasileiras, em consonância analisar os impactos gerados mediante a aplicação da LGPD no cenário do sistema de segurança da informação, visando se adaptar à regulamentação estabelecida pela Lei Geral de Proteção de Dados Pessoais. Este trabalho faz um estudo da Lei, bem como suas características e padrões, com o propósito de apontar as suas necessidades, parâmetros de execução e aplicações, analisar quais as implicações da LGPD em ambientes corporativos, identificar e catalogar as ameaças a privacidade dos dados na atual sociedade, bem como o impacto da padronização.

Para tanto, a pesquisa bibliográfica de cunho qualitativa - descritiva sobre o assunto foi desenvolvida, utilizando palavras-chave como guia de busca. Os resultados da pesquisa mostram fatores de fracasso no âmbito das MPEs aos empreendedores e incentivos para

maximizar oportunidades de sucesso, assim ficando menos suscetível ao encerramento precoce das atividades, proposta da LGPD na gestão da segurança da informação relacionada às ameaças encontradas nos hábitos e processos das organizações.

2. MICROEMPRESA: CONCEITOS E DEFINIÇÕES

Pouco ainda se sabe sobre a origem das pequenas empresas brasileiras, embora pequenas e médias empresas sejam alvo de diversos trabalhos de pesquisa. Prado Jr (1945) destacou que, no início do século 16, existiam apenas grandes indústrias fábricas de açúcar que eram viáveis na China. Para os autores citados, os pequenos direitos de propriedade sempre foram e existem desde as atividades de produção colonial.

Em 1785, devido à crise de abastecimento, a demanda era tão grande para abertura de pequenas empresas algodoeiras que se tornou necessário proibir o cultivo de algodão. Levando pequenos agricultores a replantar mandioca e outros alimentos. Segundo Palácios (2002), as pequenas empresas brasileiras são grandes economias, não apenas antecedentes atividades de apoio.

Foi só no século 19 que os pequenos direitos de propriedade começaram a decolar devido ao crescimento populacional, à desintegração da administração civil, ao enorme sistema de exportação e ao declínio de certas partes do País. O Desenvolvimento de larga escala em Santa Catarina, Rio Grande Sul e Paraná (PRADO JR., 1945). O primeiro lote de MPEs localizava-se em São Paulo e funcionava nos seguintes departamentos: Manufatura, serviços, agricultura, transporte e comércio. Nas décadas de 1970 e 1980, devido ao grande número de desempregados, as pequenas empresas tornaram-se uma importante substituta para contratação de mão de obra, com abertura de pequenas e microempresas e aproveitamento na economia brasileira. Esse período passou a ser conhecido como o "milagre econômico" (SILVA et al., 2012).

Os conceitos de microempresa e microfinanças foram lançados em 1976 pelo ganhador do Prêmio Nobel Muhammad Yunus, fundador do Grameen Bank (Banco do Rural), em Bangladesh. O banco foi criado com o objetivo de fazer pequenos empréstimos aos pobres, principalmente mulheres, para ajudá-los a obter autossuficiência econômica. O princípio fundamental por trás do Grameen Bank é que o crédito é um direito humano. Essa estratégia foi altamente eficaz à medida que o banco cresceu exponencialmente; de menos de 15.000 mutuários em 1980, o Grameen Bank passou a ter 2,34 milhões de membros em 1998, 7,67 milhões no final de 2008, 97% dos quais são 9,4 milhões de mulheres hoje.

Uma microempresa é geralmente definida como uma pequena empresa que emprega entre 10 ou menos empregados e tem um balanço ou faturamento inferior a um determinado montante (por exemplo, até meio milhão). A maioria dos proprietários de microempresas está principalmente interessada em ganhar a vida para sustentar a si e às suas famílias. Eles só fazem o negócio crescer quando algo muda na vida deles e precisam gerar uma renda maior. De acordo com informações encontradas no site Census.gov, as microempresas representam 95% dos 6,4 milhões de empresas brasileiras rastreadas pelo censo.

Diz-se que as microempresas agregam valor à economia de um país, criando empregos, aumentando a renda, fortalecendo o poder de compra, reduzindo custos e agregando conveniência aos negócios. Como as microempresas normalmente têm pouco ou nenhum acesso ao setor bancário comercial, muitas vezes dependem de "microempréstimos" ou microcrédito para serem financiadas. Uma empresa que é considerada micro ou pequena empresa (MPE) no Brasil tem algumas restrições básicas, por exemplo, o status de se incluir ao Simples Nacional. Atualmente, existem pelo menos três definições usadas para restringir pequenas ou microempresas.

O NEIS (New Enterprise Initiative Scheme) é um programa governamental na Austrália que ajuda pessoas desempregadas a iniciar seus próprios negócios. Embora não seja especificamente para

microempresas, muitas, senão a maioria das empresas iniciadas neste programa, são microempresas (no sentido de ter capital limitado e apenas uma pessoa envolvida no negócio).

O campo da microempresa tem uma história de 20 anos nos Estados Unidos. Embora o termo "microempresa" já tenha sido usado internacionalmente no final dos anos 1970, ele passou a ser usado internamente nos Estados Unidos cerca de uma década depois. Tradicionalmente, o setor empresarial era classificado em três grupos: grande, médio e pequeno. A U.S. Small Business Administration (SBA) define uma pequena empresa como a que tem até 500 empregados. Em 1991, a SBA reconheceu a microempresa como uma categoria de negócios separada ou distinta.

As microcréditos podem ser usados para despesas gerais de negócios, como capital de giro e ativos tangíveis, como estoque, móveis e equipamentos. Eles não podem ser usados para pagar o proprietário da microempresa, para comprar imóveis, pagar dívidas existentes ou para entidades sem fins lucrativos não qualificadas.

Durante a década de 1990, o campo da microempresa cresceu rapidamente. Começando com um pequeno número de organizações sem fins lucrativos, testando modelos de países em desenvolvimento, o campo agora tem prestadores de serviços em todos os estados, uma associação comercial nacional (ACN), um número crescente de associações estaduais e intermediários de financiamento, e várias pesquisas e políticas organizações. O Instituto Aspen e o FIELD (Fundo da Microempresa para Inovação, Eficácia, Aprendizagem e Disseminação) coletam dados sobre as organizações da área desde 1992. O primeiro diretório, em 1992, listou 108 organizações que se identificaram como trabalhando na área. Em 2010, esse número havia crescido para mais de 800 organizações que fornecem serviços diretos a empreendedores, seja microfinanciamento, seja serviços de desenvolvimento de negócios.

As Instituições Financeiras de Desenvolvimento Comunitário (CDFIs), especialmente os Fundos de Empréstimos para Desenvolvimento Comunitário, frequentemente oferecem capital

de empréstimo para microempresas nos Estados Unidos. Anthony Hilb, autor de Make Money with a Microbusiness e fundador da microbusinessowners.com, afirmou: "As microempresas existem desde que as pessoas trocaram bens e serviços em suas comunidades. Hoje, as microempresas podem ter um impacto muito maior; produtos e serviços podem ser trocados em volumes, distâncias e velocidades nunca imaginadas. O crédito aqui se deve aos avanços na tecnologia. Com a internet, aplicativos e outras tecnologias disponíveis (geralmente de graça), as microempresas continuarão a explodir em popularidade.

3. DESENVOLVIMENTO EM PEQUENAS E MÉDIAS EMPRESAS

Rápidas mudanças tecnológicas vêm aumentando a complexidade e turbulência do ambiente de negócio. A crescente lacuna entre os requisitos de negócios e o conhecimento adquirido em educação formal são apenas alguns dos fatores que se impõem às empresas, independentemente do porte. Estas necessitam de formação e desenvolvimento contínuo dos empregados. O investimento em treinamento e desenvolvimento dos empregados é um indicador-chave para entender o que está acontecendo nos negócios de hoje e concorrência.

O desenvolvimento empresarial e o desenvolvimento do pessoal estão diretamente ligados. Em outras palavras, uma empresa não pode ser desenvolvida sem o desenvolvimento de seus recursos. A concepção e implementação de um sistema eficaz de treinamento e desenvolvimento é um desafio para as pequenas e médias empresas, pois tais programas geram custos no presente, enquanto quase todos os resultados potenciais de treinamento e desenvolvimento resultarão no futuro. No entanto, a crescente complexidade e escopo de trabalho, desenvolvimento contínuo de tecnologias, e intensa competição fazem o treinamento e desenvolvimento dos empregados necessários.

Além disso, empregados treinados fornecem uma vantagem competitiva para a empresa que, uma vez adquirida, não é fácil de

ser copiada pelos concorrentes. Independentemente do tamanho da empresa, o treinamento deve ser realizado de forma sistemática. Por exemplo, a análise das necessidades de treinamento e do plano de desenvolvimento deve ser a base para a decisão sobre o treinamento dos empregados. As pequenas e médias empresas muitas vezes não apresentam análise das necessidades de treinamento e tomada de decisões relacionadas a essas questões. Geralmente, empregados em MPEs têm muito menos probabilidade de receber treinamento do que empregados em organizações maiores. (Hatten, 2012).

De acordo com Patton (2005), críticos fatores que limitam as pequenas organizações a se tornarem mais engajadas na área de treinamento e desenvolvimento de pessoal são falta de tempo e recursos financeiros. Os proprietários de negócios muitas vezes não são cientes dos benefícios e efeitos do treinamento e desenvolvimento, e não estão familiarizados com métodos de treinamento disponíveis.

Mazur e Coleman (2008) sugerem a mentoria como uma forma de treinamento e desenvolvimento de trabalhadores mais jovens e menos experientes. Trata-se de uma solução eficiente para pequenas organizações. Esta abordagem para o desenvolvimento da equipe seria focada em ambas as necessidades dos empregados e as necessidades da empresa. Além de orientação útil, os métodos de desenvolvimento dos empregados são a extensão e a rotação de cargos.

Em pequenas e médias empresas, treinamento e desenvolvimento de proprietários e/ou gerentes são muito importantes. Treinamento e os programas de desenvolvimento para proprietários/gerentes devem cobrir uma ampla gama de tópicos em finanças, contabilidade, marketing, empreendedorismo e gestão (liderança, motivação, comunicação) porque esse conhecimento recém-adquirido pode facilitar significativamente o processo de tomar boas decisões de negócios.

4. OS CANAIS DE COMUNICAÇÃO: A IMPORTÂNCIA DA COMUNICAÇÃO

Entre a maioria de suportes para formação empreendedora disponíveis no Brasil, poucos dão grande importância para a comunicação empresarial e, paralelamente a isso, segue na cabeça de muitos pequenos empresários a ideia errada de que o uso das ferramentas de comunicação, incluindo a publicidade, é para grandes empresas. Esse pensamento pequeno pode levar um negócio à falência.

Por isso, há a importância de fortalecer o conhecimento em comunicação. A comunicação é antiga e, desde seus primórdios, é uma ferramenta que integra as pessoas e as diversas atividades realizadas diariamente, principalmente nas empresas. Hoje, diante das exigências do mundo dos negócios, é fundamental que ela ocorra de forma alinhada e eficaz, posicionando bem a empresa no mercado.

Nos últimos anos, a comunicação tem sido considerada a principal ferramenta estratégica das relações profissionais e sociais, pois exerce um extraordinário poder para o equilíbrio, o desenvolvimento e a expansão das empresas. O processo comunicacional se estende ao cenário externo e, internamente, permite que gestores e empresários exerçam as funções de planejamento, organização, liderança e controle das ações e operações envolvidas, transmitindo informações sobre seus produtos, mercadorias e serviços de forma eficaz, a clientes externos e internos. (CARRASCO; IBTA, 2010)

Importante mencionar que há necessidade de conhecimento por parte do comunicador referente ao mercado no qual a organização está inserida, o perfil dos consumidores com quem a empresa se relaciona e, principalmente, dos canais utilizados para promover este relacionamento. Uma boa alternativa para se conhecer o mercado é por meio do plano de negócios, um poderoso instrumento para traçar um retrato fiel do mercado, do produto e das atitudes do empreendedor. (SEBRAE,2010)

O comunicador deve estar atento a todos os acontecimentos que estão à sua volta. Principalmente, deve estar em sintonia com as novas tecnologias, sendo capaz de realizar uma comunicação eficiente. (BUENO,2003,p.12)

Além de conhecer o mercado, é extremamente importante conhecer a empresa e seu negócio e, uma excelente alternativa para se conseguir mensurar um negócio é por meio de um bom planejamento estratégico, que dá uma boa definição do propósito da empresa, facilitando a inserção de seus produtos e serviço no mercado. O planejamento estratégico serve de referência e guia para ações organizacionais.

Tanto o plano de negócios quanto o planejamento estratégico são instrumentos totalmente acessíveis em se tratando de micro e pequenos negócios. A sua importância se estende ao processo organizacional, auxiliando diretamente na comunicação empresarial por proporcionar conhecimento sobre o negócio e o mercado. A comunicação é um fator que se soma às estratégias, sendo imprescindível para qualquer organização. Muitas vezes, a marca de determinado produto passa a valer mais do que as próprias fábricas, equipamentos e bens das empresas.

5. COMUNICAÇÃO PARA MICRO E PEQUENAS EMPRESAS

No Brasil, onde as dificuldades em gerir e manter um negócio são grandes, o que resulta em incertezas, os empresários precisam ficar atentos não somente às vendas, mas também na comunicação dessas empresas. Na constante luta pela sobrevivência, as pequenas empresas enfrentam competidores de todos os portes. Alguns até com potencial bem mais competitivo, no que diz respeito aos preços, distribuição e até mesmo na comunicação da marca. As micro e pequenas empresas, embora normalmente capazes de criar excelentes produtos e/ou serviços para atender a seus consumidores, não teriam sucesso se esses não fossem conhecidos e desejados pelos seus clientes.

Toda organização, incluindo as micro e pequenos negócios, precisa se comunicar de alguma maneira, afinal é necessário mostrar os produtos e despertar o interesse do público-alvo. A melhor maneira de se divulgar produtos, serviços e, principalmente, a empresa, é por meio da publicidade. Porém a publicidade é bem aceita em uma empresa quando feita em conjunto com uma visão estratégica e gerencial que envolva desde um bom plano de negócios a um bom planejamento estratégico. (GARCIA et al., 2006)

Para Maria Tereza Garcia, Fábio Caim, Silene de A. G. Lourenço, Tânia Trajano (2006, p.75), publicidade se define da seguinte maneira: Publicidade é a atividade de divulgar comercialmente um produto, serviço, uma marca ou ideia de maneira planejada, organizada, remunerada e mensurável, por meio de comunicações direcionadas a um público-alvo, tendo como objetivo a lucratividade e usando, para isso, os meios de comunicação disponíveis e adequados aos objetivos das ações publicitárias.

A publicidade é uma ferramenta que serve para gerenciar a comunicação de um empreendimento e, em conjunto com outras ferramentas, aliada a uma comunicação interna, ajuda a construir uma imagem de marca forte no mercado, e, sobretudo, expor com eficiência o que a empresa tem a oferecer. Os restaurantes, por exemplo, são identificados por fachadas e divulgam suas especialidades ao cliente por meio de cardápios. Essas duas peças são produções da comunicação da empresa, assim como guardanapos com o logotipo do estabelecimento, uniforme dos garçons, sinalizações no ambiente (banheiro masculino, feminino), etc. (GARCIA, 2006, p.76)

Todos estes materiais citados por Garcia são considerados peças de comunicação porque foram realizadas dentro de um propósito ideológico construído pela empresa e de maneira organizada cumprem o objetivo de atrair clientes para consumirem seus produtos e serviços.

O primeiro passo para se trabalhar com as ferramentas de comunicação é a criação de uma marca, que reflita as características da empresa, cumprindo o objetivo de defender os produtos e/ou serviços da empresa. Ela é a primeira forma de contato do consumidor com a

organização. Mais do que isso, a marca tem a finalidade de diferenciar a empresa das demais, podendo inclusive interferir positivamente na lealdade do consumidor, na medida em que confere visibilidade por meio de identidade e personalidade, facilmente reconhecidas e distinguíveis.

A construção de uma marca forte deve ter como objetivos a diferenciação, proximidade, empatia, confiabilidade, segurança e desejo. O ideal é que a marca traduza um conceito forte para sua organização, refletindo o conjunto de tudo aquilo que há de mais importante na empresa. Ela é estabelecida por meio de um logotipo, um grafismo que simboliza uma personalidade, um conceito, critérios de atuação, uma missão, certos valores e comportamentos relacionados ao negócio da organização. É a junção de valores tanto racionais quanto emocionais. (GARCIA et al., 2006).

Segundo Garcia 2006, para compor a identidade da marca é preciso pensar nos seguintes itens: 1- Missão e principais valores da empresa; 2- Foco do negócio; 3- Diferenciais; 4- Imagem a ser projetada (personalidade da marca); 5- Principais formas e cores; 6- Logotipo ou símbolo (elementos que poderão ser usados como assinatura em qualquer peça da empresa); 7- Slogan (frase curta, objetiva e de impacto que sintetiza as características da empresa/produto para o consumidor). Garcia reforça ainda que as primeiras informações necessárias para composição da identidade da marca são encontradas no planejamento estratégico, afirmando a importância de investir na criação de um bom planejamento estratégico, além de um bom plano de negócios.

6. AS MÍDIAS OU CANAIS DE COMUNICAÇÃO MAIS ADEQUADOS PARA MICRO E PEQUENAS EMPRESAS

Diante da importância da micro e pequena empresa para sustentação do país, e diante da grande importância da comunicação para o desenvolvimento e crescimento de qualquer empreendimento, o grande desafio é encontrar, caso exista, um veículo de comunicação

que mais se adapta às características das micro e pequenos empreendimentos.

Em entrevistas realizadas com diversos profissionais da área de comunicação foi possível perceber a carência de conhecimento acerca da comunicação e sua importância para as micro e pequenos negócios. Entre os entrevistados, Antonio Viegas, analista de comunicação do Sebrae Nacional, acredita que não exista uma mídia mais adequada para MPE. Segundo ele, a mídia varia de acordo com o tipo de negócio.

Porém, em se tratando de comunicação para micro e pequenas empresas, existem certos cuidados que são essenciais, tais como: baixo custo, simplicidade. É necessário produzir uma arte que transmita confiança e credibilidade, criar uma marca adequada ao tipo de negócio e até mesmo inseri-la corretamente na papelaria da empresa, ter uma boa sinalização, aproveitar a internet para se aproximar mais do público-alvo. Ele destaca a necessidade de uma boa comunicação estar atenta à comunidade, onde a empresa está inserida, e, principalmente, cultivar o boca a boca por meio de um atendimento diferenciado.

"Se as micro e pequenas empresas tivessem tudo bonitinho, uma logo bem-feita, um portfólio bem-feito, uma propaganda, mesmo que simples, mas bem-feita, ajudaria e muito no crescimento do negócio. Um exemplo recente: o senhor que fez os móveis da minha casa não tinha nenhum tipo de comunicação. Se ele tivesse um folder, um panfleto ou até mesmo um blog, seria muito mais fácil divulgar seus serviços e, dessa forma, contratá-lo. Ele precisa desse tipo de apoio, mas não sabe, ou não tem ideia de como deve agir para fazer essa comunicação. Sem contar o receio de que isso seja algo muito caro". (VIEGAS, 2010)

Viegas afirma que, infelizmente, os micro e pequenos empreendedores não estão preparados para fazer a comunicação dos seus empreendimentos, até porque sua preocupação maior é em produzir e vender para pagar suas contas. Dificilmente, ele se preocupará em fazer alguma forma de comunicação, também porque ele não conhece os veículos ou mídias que poderão ajudá-lo. Isso é

consequência da falta de investimento na educação do empreendedor e do comunicador. O Sebrae, por exemplo, não trata especificamente da comunicação em nenhum de seus principais cursos, objetiva principalmente capacitar o empreendedor para o gerenciamento e administração do seu negócio.

Entretanto, recentemente, promoveu uma oficina voltada para a comunicação, que auxilia os microempresários a promoverem seus negócios. A oficina: "Como Divulgar sua Empresa com Pouco Dinheiro", é extremamente acessível, custando R$ 20,00 reais e pode representar a inclusão da comunicação no método de preparação dos empreendedores pelo Sebrae. (SEBRAE, 2010). A cultura da comunicação ainda não foi enraizada no Brasil pelas micro e pequenos empreendedores, por isso esses empreendimentos ainda não alcançaram um patamar de sucesso que deveriam. A micro e pequena empresa precisa de apoio para fazer comunicação e se desenvolver. (Viegas, 2010)

Para Eduardo Duarte, analista de comunicação do Sebrae Nacional, as mídias dependem muito do tipo do negócio, por isso fica impossível falar de uma ou outra mídia que seja mais adequada para micro e pequenas empresas. Existe uma mídia mais adequada ao público-alvo da empresa, que varia de acordo com o tipo do empreendimento. Trata-se de adequação de público, independentemente do tamanho do negócio. A solução muitas vezes das micro e pequenos é falar diretamente com a comunidade onde está inserida a empresa, por isso a importância de se pensar bem na localização do empreendimento. (DUARTE, 2010)

Para Duarte, a solução muitas vezes dos micro e pequenos negócios é falar diretamente com a comunidade onde está inserida a empresa, por isso a importância de se pensar bem na localização do empreendimento. A comunicação da micro e pequeno empresário está muito voltada para o corpo a corpo, dependendo é claro do tipo de negócio.

Fernando Brettas, presidente da SINAPRO-DF (Sindicato das Agências de Publicidade do Distrito Federal) e sócio da G3 Comunicação,

afirma que hoje existem mídias que se adaptam a qualquer tamanho de negócio, como o rádio, que pode ser utilizado por um baixo custo. Também existem as ações promocionais de rua e a internet, em que podem ser feitos bons trabalhos por meio de marketing viral e redes sociais. Segundo Brettas, o empreendedor precisa ter cuidado com as pequenas coisas, desde a papelaria da empresa, um cartão de visitas, a uma boa marca.

Porém, não existe uma mídia que seja mais adequada ao micro e pequeno empresário. As mesmas mídias usadas por grandes corporações também podem ser usadas por pequenas empresas, logicamente que em escala menor. O importante é adaptar a mídia ao tipo de negócio, ao produto e à verba. Somente 25% das empresas têm um departamento de marketing. Se, das grandes empresas, 75% não têm um departamento de marketing estruturado, isso basta para sabermos que dificilmente uma pequena empresa o terá. (BRETTAS, 2010).

Falta treinamento para que os micro e pequeno empreendedores consigam atuar de forma correta na utilização da comunicação. Pois a comunicação publicitária exige investimentos contínuos e não produz resultados imediatos. - Os empreendedores não são capacitados o suficiente para procurar uma agência de propaganda. - Os que procuram, por falta de formação, acreditam que, fazendo um investimento qualquer, terão resultados imediatos. Entretanto, publicidade não é um produto de prateleira, é um produto customizado para cada cliente para cada empresa e para cada momento. Por isso deve ser muito bem estudado, pesquisado e planejado. - A propaganda é um processo contínuo, não existe propaganda que não seja feita dentro de um processo contínuo. (BRETTAS, 2010)

Para Brettas, é preciso que o pequeno empreendedor procure uma agência dentro do porte do seu negócio. A agência não pode ser maior que o negócio do empreendedor. Escolher uma agência de publicidade é como escolher um bom dentista, um bom arquiteto, um bom prestador de serviços. Sugere-se que o empreendedor procure uma entidade de classe que apresente uma listagem de agências de

propaganda e nela o empreendedor poderá selecionar as agências que se enquadram ao tamanho do negócio.(BRETTAS, 2010)

Como presidente da SINAPRO-DF, Brettas afirma que as agências não estão preparadas para atenderem os micro e pequenos empresários, não percebendo o grau de potencial deste segmento. As agências de propaganda estão despreparadas, hoje todos que montam uma agência buscam atingir grandes contas, o trabalho é o mesmo, mas a fatia de dinheiro é maior. Porém existe uma fatia de mercado de 90% que está desassistida, são as micro e pequenas empresas. (BRETTAS, 2010)

Bruna Machado trabalhou em agências de publicidade por 10 anos e afirma que não existe uma mídia que se adapte às características dos micro e pequenos empreendimentos. Segundo ela, a mídia é escolhida de acordo com o tipo de negócio e o público-alvo da empresa. Machado afirma que o microempreendedor tem conhecimento acerca da importância da comunicação, mas não sabe como utilizá-la. Bruna ainda afirma que as agências deveriam se especializar em atender micro e pequenos negócios, mas, infelizmente, elas só buscam grandes oportunidades de negócios. As agências não estão preparadas para atenderem às MPE. Elas querem grandes oportunidades de negócio. Mas, para isso, deveriam se especializar em micro e pequenos negócios porque poderiam crescer junto com os pequenos empresários. (MACHADO, 2010)

As micro e pequenas empresas representam as grandes oportunidades e infelizmente são pouco exploradas pelas agências. Investir no crescimento dos micro e pequenos pode ser uma grande estratégia de negócio que proporciona um crescimento conjunto entre agência e empresa.

7. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: CONTEXTUALIZAÇÃO

Com o intuito de reduzir o risco de abuso no manuseio, coleta e descarte e uso de transmissão de dados na União Europeia, em

2016, foi lançado o Regulamento Geral de Proteção de Dados (General Data Protection Regulation), estabelecendo disposições gerais sobre proteção de dados, em um novo sistema regulatório para os membros da União Europeia, substituindo a antiga diretiva 95/46 EC, de 199514 (Diretiva nº 95/46/EC. 1995) (UNIÃO EUROUA, 2016)

O GDPR serviu de catalisador para que o Brasil criasse sua própria Lei de proteção de dados pessoais, que, caso não realizasse, seria proibido de trocar dados com a União Europeia (UE). A não adaptação ao direito europeu e à agenda jurídica para se adaptar ao direito global prejudicaria alguns setores do Brasil, principalmente as empresas, prejudicando a competitividade e a inovação da economia. (BIONI, 2018)

> Por um período de dez anos, houve um debate sobre a proteção de dados em Âmbito nacional, mas legalmente não existe nenhum órgão governamental para tomar medidas disciplinares de forma completa e unificada, era feito de forma esparsa, necessitando de padronização e segurança jurídica (BIONI, 2018).

A principal resposta jurídica para questões de conectividade até então era a Constituição Federal. Em seu Art. 5º, § X, a Constituição da República Federativa do Brasil (CRFB) prevê a inviolabilidade da privacidade, reputação e imagem do indivíduo, com direito a danos morais e/ou material resultante de sua violação. Outras Leis, como a Lei de Acesso à Informação (LAI), Código do Consumidor (CDC), Marco Civil da Internet (MCI), Lei do Cadastro Positivo e a Lei de Crimes Informáticos também eram usados em alguns casos e situações de violação de dados pessoais (DONEDA, 2011).

O CDC aponta direitos básicos do consumidor, como práticas comerciais utilizadas para coleta de dados, alguns casos classificados como abuso no contexto (BLUM, 2020). O MCI manifestou preocupação com a tutela de privacidade e segurança dos dados pessoais e segurança, ao restringir o uso ou acesso de informações confidenciais na internet,

sem violar a privacidade, respeito às regras de uso, privacidade no fluxo de comunicação pela internet; manter e criar logs de acesso de aplicativos de internet disponíveis, guarda e disponibilização em manter a intimidade, honra e imagem dos envolvidos (DONEDA,2011).

Na sociedade da informação, o desenvolvimento de estratégias de marketing e tecnologia apresenta simultaneamente vantagens e desafios para a proteção dos direitos fundamentais. Portanto, fica claro que as Leis existentes no País não são suficientes para proteger a privacidade, a imagem e honra das pessoas, intimidade e os problemas emergentes que surgiam. (BRANCO, 2017)

O MCI, no Decreto nº 8.771/2016, introduziu o conceito de dados pessoais, mas não especifica a definição de dados sensíveis. Nessa situação em que os dados não têm limites, o Brasil precisava criar uma agenda urgente sobre a Lei Geral de Proteção de Dados Pessoais, para atender países que já possuem Leis precisas e eficazes (Lei Federal nº10.406, 2002).

O caminho para o modelo atual teve início em 2010, com o tema tendo a primeira consulta pública realizada pelo Ministério da Cultura. No início de 2011, as empresas e a população local contribuíram para a discussão inicial, propondo regulamentação da Lei nacional de proteção de dados pessoais (BRAZIL, MINISTÉRIO DA CULTURA, 2018).

Vazamentos feitos por Edward Snowden em 2013 revelaram em detalhes um programa secreto de vigilância dos EUA e vigilância de tráfego em todo o mundo sobre tráfego de informação e comunicação de diversos países, levando a lugares como o Brasil e Europa alertas e preocupações sobre seus dados pessoais. Então, para acelerar o Processo de aprovação do Marco Civil da Internet (MCI), visto como um acerto no sistema de proteção de dados pessoais. No entanto, ainda havia necessidades de preencher algumas vagas não resolvidas na MCI (EWEN MACASKILL, 2013).

Com a segunda consulta sobre este tema em 2016, foi gerada uma comissão especial que fornecia pareceres sobre uma proposta legislativa. Algumas empresas nacionais e organizações internacionais

da época contribuíram para o amadurecimento das ideias. Quando o GDPR entrou em vigor em maio de 2018, em que substituiu a antiga orientação, o Brasil via a necessidade de uma Lei semelhante. Visto que esta dispõe de padrões em que apenas fluxos de dados internacionais podem estar disponíveis, se outros países possuírem Leis de proteção de dados relevantes como na Europa.

Se aprovadas por votação na reunião do Senado estadual de julho de 2018, as mudanças no MCI protegeriam melhor os dados pessoais no Brasil e regulariam como eles podem ser gerenciados e coletados. Incluindo de certa forma o Brasil na lista de países com Leis semelhantes e específicas por assunto (BNDES, 2016). Sancionada em 14 de agosto de 2018, a Lei Federal nº 13.709, conhecida como LGPD, passa a vigorar no final de 2020. A Lei trata de uma série de pontos que ainda não estão contemplados na Lei ou de uma pequena quantidade de pontos na Lei. A compilação em 65 artigos estabeleceu a forma como as empresas devem gerenciar os dados e proteger a privacidade dos indivíduos (BRASIL, 2018).

> A Lei Nº. 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), foi criada com base no Regulamento Geral de Proteção de Dados (GPDR), que é sobre privacidade e proteção de dados pessoais, aplicável a todos na União Europeia (MACIEL, 2019).

A LGPD foi aprovada pelo ex-presidente Michel Temer e entrou em vigor a partir de 16 de agosto de 2020 para regular atividades e tipos de tratamento sobre dados pessoais no Brasil. O Brasil possui uma série de Leis e regulamentos relativos à proteção e privacidade de dados, como o Marco Civil da Internet, o Código do Consumidor, criando um cenário com várias Leis e um quadro jurídico complexo. LGPD substitui esta situação complicada com muitas diretrizes, regras e regulamentos específicos para o uso, proteção e transferência de dados pessoais para o Brasil.

A LGPD altera o Marco Civil da Internet no Brasil, que agora inclui o termo privacidade em seu ordenamento jurídico (SÁ, 2019). De acordo com art. 1º da LGPD (Lei nº 13.709, de 14 de agosto de 2018), a Lei aplica-se a todo e qualquer processamento de dados, por qualquer meio, mesmo que seja feito por uma única pessoa física ou jurídica de direito público ou privado

> Art. 1º. A legislação regula o tratamento de dados pessoais, incluindo meios digitais, por pessoa física ou jurídica de direito público ou privado, com a finalidade de proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da humanidade. (BRASIL, 2018)

A LGPD é baseada nos direitos fundamentais à liberdade e privacidade, como a livre iniciativa e o desenvolvimento econômico e tecnológico do País, segundo Art. 2º da Lei nº 13.709, de 14 de agosto de 2018. A Lei estabelece todas as informações que identifiquem diretamente o proprietário ou ajudem a naturalizar a identidade de uma pessoa e identificá-la, como dados pessoais, e quaisquer processos realizados em dados pessoais, como coleta, uso, acesso, transferência, processamento, arquivamento e transferência, nos termos do artigo 5º da Lei Nº. 13.709, de 14 de agosto de 2018 (BRASIL, 2018).

A Lei exige que as atividades de processamento de dados pessoais sejam compatíveis com os seguintes princípios: propósito, adequação, necessidade, acesso livre, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilidade e contribuição, Art. 6º da Lei nº 13.709 de 14 de agosto de 2018 (BRASIL, 2018). Com a LGPD, todas as instituições brasileiras, independentemente de seu porte, devem investir em segurança tecnológica para evitar violações de dados pessoais (ROCHA, 2019).

8. PRINCIPAIS ASPECTOS DA LGPD

A proteção de dados está diretamente ligada à cultura da internet, portanto, em razão disso é implementada a Lei Geral de Proteção Dados Pessoais (LGPD) (Lei nº 13.709/2018). Dessa forma, é um documento que almeja promover uma cultura de proteção de dados, tanto para pessoas jurídicas quanto físicas, e é regida pela informação e privacidade para autodeterminação (art. 2, § I e II). Nesse contexto, as novas políticas de ética e educação informacional como meio de proteção do público contra o crime cibernético. (BRASIL, 2018)

A seguir, serão listados os principais pontos destacados na LGPD:

- **Dados pessoais:** De acordo com a LGPD, todas as informações que identificam, direta ou indiretamente, uma pessoa viva são dados pessoais, tais como: RG, CPF, nome, sexo, data e local de nascimento e endereço residencial, telefone, localização (GPS), foto, registro de saúde, renda, cartão bancário, renda, hábitos de consumo, preferências de entretenimento, endereço, etc.
- **Consentimento individual:** O consentimento é um ponto muito importante dentro da LGPD. Portanto, é a base de dados do usuário que deve ser tratado. No entanto, existem exceções. Se for importante cumprir os requisitos legais, é possível processar os dados sem consentimento.
- **Garantia à pessoa física e jurídica:** A LGPD traz diversos direitos à pessoa física, como retirar o consentimento e transferir os dados para outro prestador de serviço, possibilitando a solicitação de exclusão de dados, correção de dados, portabilidade de dados, informações sobre a possibilidade de não consentir com o tratamento e consequhências negativas, de informações sobre o compartilhamento de dados pessoais.
- **Agentes responsáveis e supervisão central:** A Autoridade Nacional para Proteção de Dados Pessoais (ANPD) é

responsável por punir e supervisionar em caso de não cumprimento da Lei. As organizações devem ter certos agentes para controlar, operar e gerenciar tratamento de dados, dependendo do seu volume e tamanho. É necessário que administradores da base de dados pessoais de empresas que realizam a gestão de riscos e falhas foquem na tomada de medidas preventivas, documentando Padrões de governança, com replicação das melhores práticas e certificações existentes em mercado. Devem organizar pesquisas, preparar planos de emergência e resolver incidentes com habilidade. Cobrindo tudo com transparência e com a responsabilidade de notificar a ANPD e os cidadãos afetados quando ocorrer um vazamento de dados.

- **Penalidades:** Negligência e falta de segurança na proteção de dados pessoais dos usuários resultarão em multas altas. Organizações e os subcontratados que tratarão dados são solidariamente responsáveis por qualquer dano causado. A ANDP define o nível de penalidade de acordo com gravidade da falha enviando avisos e instruções com antecedência para aplicar sanções. As multas chegam a 2% do faturamento anual da empresa e, no Brasil, dentro do limite de R$ 50 milhões por infração.

9. PRINCÍPIOS GERAIS DA LGPD

A aplicação da Lei Geral de Proteção de Dados Pessoais é dirigida ao indivíduo jurídico e físico, visto que os dados individuais estão nos bancos dos órgãos públicos e também em empresas. A Lei destina-se a proteger os direitos fundamentais de liberdade e da privacidade e o livre desenvolvimento da personalidade natural. **Dessa forma, podemos dizer que a LGPD não é aplicável:**

- Nos dados oficiais de pessoa jurídica, já fornecidos no setor intelectual.

- Processamento de dados pessoais por uma pessoa física para fins econômicos, jornalísticos, privados, artísticos ou educacionais.
- Para proteger o público, proteger o país, fins de segurança do estado ou a investigação e repressão de infrações penais.
- Nos dados de pessoas mortas e dados em transporte, ou seja, aqueles não destinados a Agentes de Tratamento no Brasil.

A LGPD se aplicará aos dados processados no âmbito da zona de proteção em território brasileiro, ainda que envolva pessoa estrangeira. É possível notar que GDPR e LGPD possuem mais semelhanças entre si do que pontos de diferença. Os dados pessoais devem ser relevantes, limitados e suficientes em relação às finalidades específicas para as quais são processados. Isso fornece garantia, evitando assim o uso ilimitado dos dados pessoais coletados, de várias maneiras que os proprietários dos dados podem esperar (LORENZON, 2021)

No artigo 6.º, a Lei Geral de Proteção de Dados cita os seus princípios para dirigir o tratamento de dados pessoais (BRASIL, 2018):

- **Princípio da finalidade:** é muito importante para a proteção de dados pessoais, para consentir com a divulgação de dados pessoais, se não estiver visível para o Operador ou Controlador. Legalmente, o objetivo é realizar o processamento para determinados fins legítimos e transparentes sem a possibilidade de processamento adicional de maneira assíncrona para esses fins. Não é permitido aos agentes de tratamentos utilizar os dados pessoais dos usuários que excedem a finalidade notificada ao interessado antes da coleta de dados. Ele vincula o Controlador de dados, que indica claramente a finalidade do tratamento dos dados, com penalização a reconhecer o comportamento ilegal com base em objetivos amplos. (Rossnagel,2003, p.140).
- **Princípio da suficiência:** Define qual processamento de dados deve ser consistente com o propósito comunicado ao

proprietário. Assim, os Controladores e os Operadores não podem usar dados que não correspondam à finalidade alvo pretendida. (DONEDA, 2006)

- **Princípio da necessidade:** Os limites do mínimo necessário para a realização de tratamento para seus objetivos. Inclui dados relevantes, igualmente e não excessivamente, pois desafia o propósito do tratamento de dados.
- **Princípio do acesso livre:** permite que o proprietário obtenha sua cópia gratuita de dados coletados e como seus dados são processados pelo Controlador, que deverá cumprir o prazo máximo de 1 (um) mês. Garantindo ao mesmo tempo o direito de corrigir e adicionar seus dados pessoais, ou mesmo removê-los se não forem importantes (DONEDA, 2006).
- **Princípio de Qualidade de Dados:** Requer banco de dados consistente, eles são tratados de forma justa e imparcial, não excessivamente e adequadamente em paralelo de acordo com o objetivo declarado, e, claro, preciso e atual. Nesse caso, esta política inclui cancelamento de dados, direito de acesso e retificação. O acesso dá a uma pessoa o direito de acessar informações sobre si mesma registradas quando necessário (CUEVA, 1990). E o cancelamento, uma vez que a correção visa garantir a qualidade dos dados, para que possam ser cancelados ou removidos em caso de erros.
- **Princípio da transparência:** O princípio da transparência nas organizações estipula que estas devem dar muita informação para a pessoa em relação a processamento de informações pessoais, que deve ser conciso, acessível, transparente, claro e facilmente acessível ao titular dos dados. O objetivo da política é aberto para que possa evitar abusos cometidos por agentes.
- **Princípio de segurança e prevenção:** O princípio de segurança e prevenção concentra-se em determinar se todos os dados serão processados em um para garantir a

segurança adequada, não autorizada ou ilegal. Estabelece proteção contra danos, perdas e riscos, usando estratégias organizacionais apropriadas. Por agentes de tratamento está ligado a medidas preventivas para evitar possíveis danos para o processamento de dados pessoais. Dessa forma garante a prevenção contra ou qualquer dano decorrente do processamento de dados pessoais.

- **Princípio da não discriminação:** Estabelece que o processamento de dados não deve feito para fins de discriminação ilegal ou abusiva. Não pode haver limitação dos titulares de dados pessoais durante o processamento de seus dados por características (raça, nacionalidade, opinião política, religião/crença, localização, filiação sindical, condição genética, saúde ou condição sexual). Tal exclusão só é possível nas circunstâncias específicas previstas em Lei.
- **Princípio da prestação de contas e responsabilidade:** visa garantir a reparação justa e completa por danos materiais e morais ao indivíduo devido à violação do seu direito à privacidade. O agente administrativo de dados pessoais deve introduzir medidas apropriadas e adequadas para provar a conformidade com a LGPD.

10. CONCEITO E DEFINIÇÃO DE DADOS NA LGPD: CLASSIFICAÇÕES

De acordo com a LGPD, os dados podem ser classificados da seguinte forma, categorias.

a) Titular dos Dados

É uma pessoa singular a quem os dados se referem, identificável e reconhecível. Possibilitando a identificação direta ou indireta do titular dos dados pessoais. A LGPD traz no artigo 18 nove dispositivos em favor do direito do titular já mencionado no artigo 5º (BRASIL,

2018). "Art. 18º. O titular de dados pessoais tem o direito de receber do Controlador, em relação aos dados do titular por ele processados, a qualquer momento e mediante solicitação:

> I - confirmação da presença de tratamento; II - acesso aos dados; III - correção de dados incompletos, incorretos ou desatualizados; IV - anonimato, bloqueio ou eliminação de dados desnecessários, excessivos ou processados em desacordo com o disposto nesta Lei; V - a portabilidade de dados para outro prestador de serviço ou produto, quando expressamente solicitado, nos termos da legislação das autoridades nacionais, para proteção de segredos comerciais e industriais; VI - encerramento dos dados pessoais processados com o consentimento do titular, ressalvados os casos previstos no art. 16º desta Lei; VII - informações sobre organizações públicas e privadas com as quais o Controlador utilize os dados em conjunto; VIII - informação sobre a possibilidade de não consentir e as consequências da recusa; IX - retirada do consentimento, nos termos do § 5º do art. 8º desta Lei".

b) Dados Sensíveis

São aqueles que, se roubados, podem causar danos ao titular dos dados, pois esses dados estão ligados à personalidade, caráter e dia a dia. O artigo 5º, parágrafo segundo, trata de dados sensíveis (BRASIL, 2018).

> Art. 5º Para efeitos desta Lei, considera-se dados pessoais sensíveis: dados pessoais sobre origem racial ou étnica, crença religiosa, opinião política, filiação sindical ou religiosos, filosóficos ou políticos, de saúde ou de vida, dados sexuais, genéticos ou biométricos, se vinculados a uma pessoa natural;"

c) Dados Pessoais

São aqueles que, se roubados, podem identificar uma pessoa diretamente ou indiretamente. O artigo 5º, inciso I, trata de dados sensíveis (BRASIL, 2018).

> Art. 5º Para efeitos desta Lei, considera-se dados pessoais: informações relativas à pessoa física identificada ou não.

d) Dados Anônimos

Destina-se a ocultar informações confidenciais antes que se tornem tão disponibilizados para uso. Impossibilitando saber de qual perfil é a informação. O artigo 5º, terceiro inciso, trata dos dados anônimos (BRASIL, 2018).

> Art. 5º Para efeitos desta Lei, considera-se dados anônimos: dados relativos ao titular dos dados que não possam ser identificados, tendo em conta a utilização de métodos técnicos adequados disponíveis em o momento do seu tratamento.

e) Encarregado

Sua função consiste em ações intermediárias entre titular, Controlador e ANPD, para total liberdade de processamento de dados, fiscalizar ambos, tanto o Operador como o administrador, e registrar reclamações se algo der errado. No artigo 5, § 8, trata sobre essa gestão. (BRASIL, 2018)

> Art. 5º Para efeitos desta Lei, considera-se responsável: a pessoa designada pelo Controlador e Operador para agir como um canal de comunicação entre o

> Controlador, titulares de dados e Autoridade Nacional de Proteção de Dados (ANPD).

O responsável deve ser nomeado obrigatoriamente pelo administrador, conforme artigo 41 (BRASIL, 2018).

> Art. 41º. O Controlador deve nomear um responsável pelo processamento de dados pessoais.

No entanto, deve-se notar que, no artigo 23, também revela a referência obrigatória do responsável pelo tratamento dos dados pessoais por pessoa jurídica de direito público (BRASIL, 2018)

> Art. 23º. O Processamento de dados pessoais por pessoas jurídicas de direito público aborda no art. 1º da Lei nº. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deve ser implementado para cumprir o seu propósito público, na prossecução do interesse público, para efeitos de exercício do poder de Lei ou para cumprir os requisitos Leis da função pública, desde que: o responsável seja nomeado no exercício das funções tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação prevista pela Lei nº. 13.853, de 2019) Vigência.

f) Agentes de Tratamento

O artigo 5º, inciso nove, trata dos agentes de tratamento (BRASIL, 2018).

> Art. 5º Para efeitos desta Lei, considera-se, agentes de tratamento; o Controlador e Operador;

g) Controlador

O responsável pelo tratamento é uma pessoa singular, ou coletiva, de direito público ou privado, que é responsável pelas decisões relativas ao tratamento de dados pessoais, ou seja, empresas que recebem dados de proprietários, sejam eles consumidores e/ou trabalhadores, entre outros. Os dados são recebidos pelo Controlador e configurados na estrutura de recepção, tratamento, localização e terminação de dados, passando todas as orientações para o tratamento pelo Operador.

h) Operador

O Operador é uma pessoa singular ou coletiva, de direito público ou privado, que realiza o processamento de dados pessoais em nome do Controlador. É uma pessoa funcional responsável pelo processamento dos dados na prática, que pode ser um empregado da empresa receptora/Controladora, empresa terceirizada ou mesmo um profissional autônomo. Normalmente, este Operador será alguém com experiência na área de tecnologia da informação e processamento de dados. Portanto, cabe ao Operador realizar o tratamento de acordo com as instruções fornecidas pelo regulador, que verificará o cumprimento de suas instruções e regras sobre a matéria. Controlador e Operador trabalham juntos, como agentes reais de tratamento (Art. 39) (BRASIL, 2018).

11. LGPD E SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS NAS MPE'S

Como indicado anteriormente, os dados têm alto valor prático. Por causa disso, as empresas iniciam uma busca incontrolável por essas informações. Em meio a tudo isso, há um titular de dados, que

vive uma relação desigual de vulnerabilidade. Portanto, é necessário um maior comprometimento com a autodeterminação da informação para que não haja prejuízo ao direito à privacidade e para que não sofra os efeitos da automação, que podem influenciar diretamente o seu futuro.

O melhor é a combinação entre as áreas técnica (segurança da informação) e jurídica (LGPD), pois a proteção de dados só funciona se for acompanhada de segurança da informação. Disposições legais como a LGPD regulam o conceito de autonomia e política de consentimento do usuário.

> O Art. 7º da LGPD dispõe: O tratamento de dados pessoais somente poderá ser realizado nos seguintes casos: I - mediante consentimento do titular dos dados.

Segundo Jimene (2020), a segurança da informação existia antes da necessidade de proteção de dados pessoais. No entanto, concentrou-se na proteção de informações confidenciais e estratégicas relacionadas aos negócios. É, portanto, válido afirmar este princípio "nem todos os incidentes de proteção de dados são violações de dados pessoais. Mas toda violação de dados pessoais é um incidente de segurança.

No contexto de dados pessoais, a segurança da informação é responsável por proteger o negócio de riscos e incidentes como vazamentos de dados, ataques cibernéticos e indisponibilidade. Neste caso, trata de análise de vulnerabilidades, adequação e automatização de processos, prevenção de fraudes, ou seja, funciona para que os dados não tenham uma finalidade diferente daquela para a qual foram coletados.

Segundo Jimene (2020), devem ser implementadas medidas técnicas e administrativas que permitam a proteção dos dados pessoais contra acesso não autorizado e destruição, perda, modificação, compartilhamento ou divulgação acidental ou ilegal. O atendimento

à LGPD envolve processos relacionados à tecnologia da informação, considerando o grande volume de dados armazenados em sistemas informatizados, que devem ser gerenciados com medidas e estratégias de segurança.

Além das estratégias, a segurança da informação é essencial para proteger o conjunto de dados de uma empresa, pois seus métodos visam viabilizar e garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações. É importante para qualquer empresa conhecer seus dados e restringir o acesso, além de saber para onde são transferidos, armazenados, compartilhados.

A utilização de recursos técnicos que viabilizem a segurança da informação no ambiente digital é necessária para cumprir as obrigações legais de tratamento de dados pessoais e para garantir a privacidade dos titulares dos dados. Alguns exemplos de tecnologias que contribuem para a segurança das informações e, consequentemente, para a proteção dos dados: ferramentas de autenticação de acesso, serviços de criptografia, assinatura digital e certificado digital (JIMENE, 2020).

Por isso, é importante estar atento à situação em que estamos presos à superestimação de dados pessoais e à grande interação dos usuários, a fim de criar uma cultura de gestão da segurança da informação no Brasil. Esta é a única forma de respeitar efetivamente os direitos fundamentais e reduzir o risco de ataques e uso indevido de dados pessoais.

12. MÉTODOS PARA PROTEÇÃO DOS DADOS DE EMPRESAS POR MEIO DA LGPD

Para obter o consentimento efetivo e eficiente, a LGPD estabelece princípios a serem observados, limita a coleta de dados e cria obrigações para que a empresa atue sempre de acordo com o consentimento do usuário. Se não cumprir suas instruções, a agência será responsabilizada. Entre eles estão:

> Advertência, multa ou proibição total ou parcial de atividades relacionadas ao processamento de dados. As multas podem variar de 2% da receita do ano anterior até R$ 50 milhões, incluindo multas diárias. A Lei prevê ainda a obrigação de divulgação de eventos, o apagamento de dados pessoais e a inversão do ónus da prova a favor do titular dos dados. (SA, 2019, p. 18).

Também estabelece os direitos dos titulares dos dados, de acordo com a LGPD, em seus artigos 9º e 18º:

> Art. 9º O titular dos dados tem o direito de facilitar o acesso à informação sobre o tratamento dos seus dados, que deve ser disponibilizada de forma clara, adequada e visível no que respeita, entre outros aspetos previstos na legislação para cumprimento do princípio do livre acesso.
> Art. 18º. O titular dos dados pessoais tem o direito de obter do Controlador, em relação aos dados do titular por ele processados, a qualquer tempo e mediante solicitação: II - acesso aos dados; II - correção de dados incompletos, incorretos ou desatualizados; IX - retirada do consentimento, nos termos do § 5º do art. 8 desta Lei.

Cria a Autoridade Nacional de Proteção de Dados (ANPD), cujas responsabilidades são o estabelecimento de normas técnicas, avaliação de categorias e autoridades estrangeiras quanto à proteção de dados, determinação da interpretação de relatórios de Impacto, avaliação e aplicação de penalidades, atividades de divulgação e educação sobre a Lei, e outras qualidades voltadas ao direito, aplicação da Lei e dos princípios de proteção de dados pessoais. (Lei nº 13.709/2018, Art. 55).

Com as instruções supracitadas, as empresas que realizam qualquer tipo de tratamento dos dados pessoais do usuário devem cumprir os requisitos da LGPD. Nesse contexto, esta precisarão

gastar tempo e dinheiro em programas de segurança cibernética e conformidade. No entanto, como mencionado anteriormente, a decisão legal de colocar a responsabilidade principal de dar o consentimento na pessoa não é a melhor estratégia. É nessa situação que a segurança da informação ganha destaque, pois, com seus fundamentos, permitirá ao usuário proteger efetivamente seus dados.

13. CONCLUSÃO

Por meio deste estudo foi possível concluir que não existem alternativas viáveis de mídias mais adequadas para MPE. Isso porque toda mídia depende de sua adequação ao negócio, produto, ao momento e ao público, ou seja, a mídia deve ser escolhida em razão do tipo do negócio, e não pelo tamanho do negócio ou por uma característica do negócio. Além disso, fica claro que a solução de comunicação para MPE não se trata da opção por uma ou outra mídia específica, mas em investir na capacitação dos micro e pequenos empreendedores, tendo em vista a sua importância, e das agências de publicidade em relação ao potencial das MPE. Neste estudo acerca da comunicação para micro e pequenos negócios, foi possível perceber o quanto é importante a comunicação para as MPE e quanto elas são importantes para o desenvolvimento do Brasil.

Este estudo, além de mostrar a relevância da comunicação para MPE, comprova a necessidade de investimento na preparação dos micro e pequenos empreendedores para que possam realizar uma boa comunicação de seus empreendimentos. Mais de 98% das empresas formais constituídas no Brasil são micro e pequenas, o que torna absurda a falta de capacitação em comunicação.

O grande desafio dos micro e pequenos negócios é encontrar mídias que se adaptem ao orçamento da empresa e que produzam resultados interessantes de divulgação do produto e da empresa, mesmo que empregando técnicas menos sofisticadas. Embora com frequência reduzida, as publicações devem ser totalmente acessíveis a todo momento e para todo o público-alvo.

As MPE precisam de agências de comunicação preparadas para atendê-las, conforme suas características, mas infelizmente ainda é difícil encontrar agências especializadas ou capacitadas para atenderem micro e pequenos negócios. A única saída para os micro e pequenos empreendimentos é encontrar pequenas agências ou agências que se adaptem ao tamanho do negócio. Apesar de não haver mídias específicas para micro e pequenos negócios, foi possível perceber que um micro e pequeno empreendimento, se bem gerido, é capaz de fazer propaganda em qualquer mídia, não com a mesma frequência que uma grande empresa, nem com a mesma proporção.

Assim, considerando todo o exposto, pode-se concluir que, em um período muito curto de tempo, os aspectos tecnológicos mudaram a vida em sociedade de inúmeras maneiras. O advento da Internet e de novas tecnologias, como câmeras portáteis e smartphones, estão removendo as barreiras físicas à comunicação.

Nesse sentido, na sociedade da informação, tudo está conectado, e os dados são gerados. Portanto, pode-se dizer que os dados se tornaram a maior riqueza da atualidade, e aqueles que têm acesso à informação podem ser considerados os donos desse sistema de poder.

Assim, dada a abrangência e gestão dos dados humanos, surgem preocupações sobre como esses dados serão utilizados. Depois, há a necessidade de controle. Passam três gerações de legislação, desde a centralização do poder inteiramente nas mãos do Estado, até à fase atual totalmente centrada no consentimento dos titulares dos dados.

A LGPD protege o processamento on-line e físico de dados pessoais de forma democrática, segura e transparente. No entanto, mesmo diante dessas regulamentações da LGPD, todos estão vulneráveis a hackers e a agentes mal-intencionados que podem violar a segurança e roubar dados pessoais.

Além disso, deve-se reconhecer que, mesmo quando o consentimento está no centro da relação de coleta e gerenciamento de dados pessoais, os usuários ainda vivem em uma relação vulnerável devido às limitações cognitivas, sua estrutura e cultura. Além disso,

o mercado está em constante mudança para criar formas de coletar dados a qualquer custo.

Assim, fica claro que a escala da assimetria informacional precisa ser sanada para uma efetiva autodeterminação da informação. Práticas gerais voltadas à proteção de dados pessoais, como a LGPD, não funcionam bem na prática. Isso porque, mesmo que tais objetos públicos exijam autonomia e consentimento, partem da ideia de que cada titular de dados é, via de regra, um sujeito livre, com capacidade razoável de compreensão do mercado de informações. Este fato é inconsistente com a realidade devido às limitações individuais e tipos de pressões de mercado, mencionadas acima.

Em última análise, é importante que o público se separe das crenças limitantes e se torne um usuário ativo e crítico, para não se tornar um indivíduo e uma massa orientadora no mercado da informação. Nesse contexto, a tecnologia pode ser introduzida na vida das pessoas para torná-la mais fácil e confortável, porém esses benefícios não devem ser colocados acima do prejuízo da privacidade. Atitudes como: limitar o escopo de publicação, negar o acesso de aplicativos ao seu site, recusar cookies se necessário, representam este importante conceito.

REFERÊNCIAS

ABREU, Karen Cristina Kraemer. Tulipas vermelhas: uma (re) Leitura das relações na (e da) Internet (p. 38 –47). IN: Synthesis –Revista de Produção Científica da FACVEST: os vários olhares da produção científica. 2004.

AMYX, C.; LORENZON, A. Online Trust: State of the Art, New Frontiers, and Research Potential. Journal of Interactive Marketing, v. 23, n. 2, p. 179–190, 2009.

ARAÚJO, J. C. (Org.). Internet & Ensino: novos gêneros, outros desafios. Rio de Janeiro: Lucerna, 2017.

BIONI, Bruno Ricardo. Proteção de dados Pessoais –A Função e os Limites do Consentimento. Rio de janeiro: Ed. Forense, 2021.

BLUM, Renato LPGD: Lei Geral de Proteção de Dados Comentada- Editora Revista dos Tribunais 2020- https://www.jusbrasil.com.br/doutrina/lgpd-lei-geral-de-protecao-de-dados-comentada/1233940129.

BRANCO, RO Cirino, S. (2017). Reflexões sobre a consciência na fenomenologia e na abordagem centrada na pessoa. Gerais: Revista Interinstitucional de Psicologia,9(2), 241-258.

BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/l13709.htm . Acesso em: 14 abr. 2024.

BRASIL. Lei n. 12.737/12. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. 2020.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Brasília. 2014. BRASIL. Lei n°7.256, de 27 de novembro de 1984. Estabelece normas integrantes do Estatuto da Microempresa, relativas ao tratamento diferenciado, simplificado e favorecido, nos campos administrativo, tributário, previdenciário, trabalhista, creditício e de desenvolvimento empresarial. Diário Oficial da União. Brasília, DF, p. 17521, 28 nov. 1984.

BRASIL. Ministério da Cultura. Gabinete do Ministro Portaria 119 28 de março de 2022 Brasília. 2022.

BRETTAS, Tatiana. Dívida pública: uma varinha de condão sobre os recursos do fundo público. In: BEHRING, Elaine; BOSCHETTI, Ivanete; GRANEMANN, Sara; SALVADOR, Evilasio (Orgs). Financeirização, fundo público e política social. São Paulo: Cortez Editora, 2012.

BUENO, Wilson da Costa. Comunicação Empresarial: Teoria e Pesquisa. Barueri: Manole, 2003. 369 p.

CAMPOS, Andre L. N. Sistema de Segurança da Informação: Controlando os Riscos. Florianópolis: Visual Books, 2006.

CHIAVENATO, Idalberto. Recursos Humanos: edição compacta. 7. ed. São Paulo: Atlas, 2002.

CARRASCO, Maria do Carmo Oliveira; IBTA, Faculdade. Conversa de Bastidor: Comunicação Empresarial.2010.

CODA, Roberto; BERGAMINI, Cecília Whitaker. Psicodinâmica da Vida Organizacional –Motivação e Liderança. São Paulo: Atlas, 1990.

CODA, Roberto. Como está o Clima? Programa de Profissionalização do Banco do Brasil. Brasília, 1998.

COETZER, A.J., Cameron, A.F., Lewis, K.V., Massey, C.L., & Harris, C. (2007). Recursos humanos.Práticas de gestão em pequenas e

médias empresas selecionadas na Nova Zelândia. Internacional Journal of Organizational Behavior, 12 (1): 17-32.

COMBS, J., Liu, Y., Hall, A., & Ketchen, D. Quanto custam as práticas de trabalho de alto desempenho Matéria? Uma meta-análise de seus efeitos no desempenho organizacional. Psicologia de Pessoal, 59 (3): 501-528.2006.

CUEVA, A. El Desarrollo Del Capitalismo em México: Siglo Veintiuno Editores, 1990

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. FERREIRA, Luís Fernando Filardi; et al. Análise quantitativa sobre a mortalidade precoce de micro e pequenas empresas da cidade de São Paulo. Revista Gestão & Produção. São Carlos, v. 19, n. 4, p. 811-823, jul. 2012.

DUARTE, Emeide Nóbrega. Conexões temáticas em gestão da informação e do conhecimento no campo da Ciência da Informação: propostas de redes humanas. Marília, UNESP, 2010. 151f. (Relatório de Pesquisa de Estágio Pós-doutoral realizado no Programa de Pós-graduação em Ciência da Informação da UNESP-Marília)

FERREIRA, J. B.; ROCHA, A; SILVA, J. F. Impacts of Technology Readiness on Emotions and Cognition in Brazil. Journal of Business Research, 2013.

GARCIA, et. Regina Leite. Niterói.UFF. Mimeo. s/d ... Petrópolis: DP et Alii, 2008, v. 1, p. 25-42 ... Rio de Janeiro: H.P Comunicação Editora, 2006.

GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. São Paulo: Atlas, 1991.

GIL, Antônio Carlos. Gestão de Pessoas: enfoque nos papéis profissionais. São Paulo: Atlas, 2007.

GILBERT, J., & Jones, G. (2000). Managing Human Resources in New Zealand Small Businesses. Asia.Pacific Journal of Human Resources, 38(2): 54-67.

GOMES, M. T. S. As Mudanças No Mercado de Trabalho e o Desemprego em Presidente Prudente/Sp –Brasil. Barcelona: Revista Eletrônica de Geografia e Ciências Sociais, v. 6, n. 119, 2002.

HATTER, Antônio Carlos. Gestão de Pessoas: enfoque nos papéis profissionais. São Paulo: Atlas, 2007

HORNSBY, J.S., & Kuratko, D.K., (1990). Gestão de recursos humanos em pequenas empresas: questões críticas para a década de 1990. Journal of Small Business Management, 28 (3): 9-18.

IBGE, INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. As micro e Pequenas Empresas Comerciais e de Serviços no Brasil 2001. Rio de Janeiro: IBGE, 2003.

JIMENE, Camilla do Vale. Da importância da segurança da informação para adequação à LGPD. In: BLUM, Renato Opice (Org.). Proteção de dados: desafios e soluções na adequação à Lei.Rio de Janeiro: Forense, 2020.

LACOMBE, Francisco. Dicionário de Administração. São Paulo: Saraiva, 2004.

LAUDON, Kenneth C.; LAUDON, Jane Price. Sistemas de Informação com Internet. Rio de Janeiro: LTC, 1999.

LIMA, Caio César Carvalho em *LGPD: Lei Geral de Proteção de Dados Comentada*. Coordenadores: Viviane Nóbrega Maldonado e Renato Opice Blum.2ª Edição. TR Revista dos Tribunais. São Paulo. 2020. pg. 181 MAZUR, L., & Coleman, A. (2008). Treinamento e Pequenos Negócios. Em habilidades críticas para o amanhã -Nosso futuro. Está em nossas mãos. Londres: Instituto de Diretores.

LORENZON, Laila Neves. Análise Comparada entre Regulamentações de Dados Pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de Enforcement. Rio de Janeiro: Law School.2021.

MARLOW, S. (2000). Investigando o uso da atividade de gestão de recursos humanos estratégicos emergentes na pequena empresa. Journal of Small Business and Enterprise Development, 7 (2): 135-148.

MARTININGO FILHO, A.; SOARES SIQUEIRA, M.. Assédio moral e gestão de pessoas: Uma análise do assédio moral nas organizações e o papel da área de gestão de pessoas. RAM - Revista de Administração Mackenzie, Volume 9, n.5, 2008, p. 11-34.

MAZUR, L., & Coleman, A. (2008). Treinamento e Pequenos Negócios. Em habilidades críticas para o amanhã -Nosso futuro. Está em nossas mãos. Londres: Instituto de Diretores.

MENEZES, Elias Jacob de Neto, DE MORAIS, Jose Luis Bolzan. Análises computacionais preditivas como um novo biopoder: modificações do tempo na sociedade dos sensores. Rio Grande do Norte: Novos Estudo Jurídicos, 2018.

NOGUEIRA, Mauro Oddo; OLIVEIRA, João Maria de. Da baleia ao ornitorrinco: contribuições para a compreensão do universo das micro e pequenas empresas brasileiras. Radar: tecnologia, produção e comércio exterior. Brasília, n.25, p. 7-18, abr. 2013.

OLIVEIRA, Wilson. Técnicas para hackers: Soluções para Segurança. Portugal: Centro Atlântico, 2013.

PALACIOS, Marcos. Ruptura. Comunicação e Novas Tecnologias no Pensamento Comunicacional Brasileiro. Pré-Conferência AIERI 2002 – Seminário O Pensamento Comunicacional Brasileiro: um panorama – 25 de julho de 2002, Porto Alegre.

PATTON, D. (2005). Treinamento em empresas menores. Em S. Marlow, D. Patton, & M. Ram (Eds.), Managing trabalho em pequenas empresas (pp. 83-108), Londres: Routledge.

PEIXOTO, Mario Cesar Pintaudi. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: Comentários à Lei 13709/2018 (LGPD) –São Paulo; Ed. Saraiva Educação, 2019.

PORTAL BRASIL. Brasileiros ficam mais tempo conectados que assistindo TV. Brasília, 2014.

PRADO JR., Caio. A Revolução Brasileira. São Paulo: Brasiliense, 6ª edição.1945.

RAPÔSO, Cláudio F L et al. LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática. RACERevista da Administração, v. 4, p. 58-67, 2019

REZENDE, Denis Alcides. Engenharia de Software e Sistemas de Informação. 3ª ed. Rio de Janeiro: Brasport, 2005.

ROCHA, I. C., Oliveira, A. M., Soares, F. I. L., Silva, G. V., Oliveira, A. M., Valdevino, R. Q. S., & Oliveira, M. C. S. (2019). A contabilidade de custos como ferramenta na formação do preço de venda em uma indústria em panificação. Brazilian Journal of Development, 5(9).

RUFINO, Nelson Murilo de Oliveira. Segurança Nacional. São Paulo: Novatec Editora, 2002.

SÁ, Marcelo Dias de. Análise do impacto da nova Lei de proteção de dados pessoais nas aplicações de internet das coisas. Brasília, 2019.

SANTOS, Dhiulia de Oliveira. A validade do consentimento do usuário à luz da Lei geral de proteção de dados pessoais: Lei n.

13.709/2018. 2019. 50 f. TCC (Graduação) - Curso de Direito, Centro Universitário de Brasília - Uniceub, Brasília, 2019.

SEBRAE. Boletim Estatístico de Micro e Pequenas Empresa. 2010.

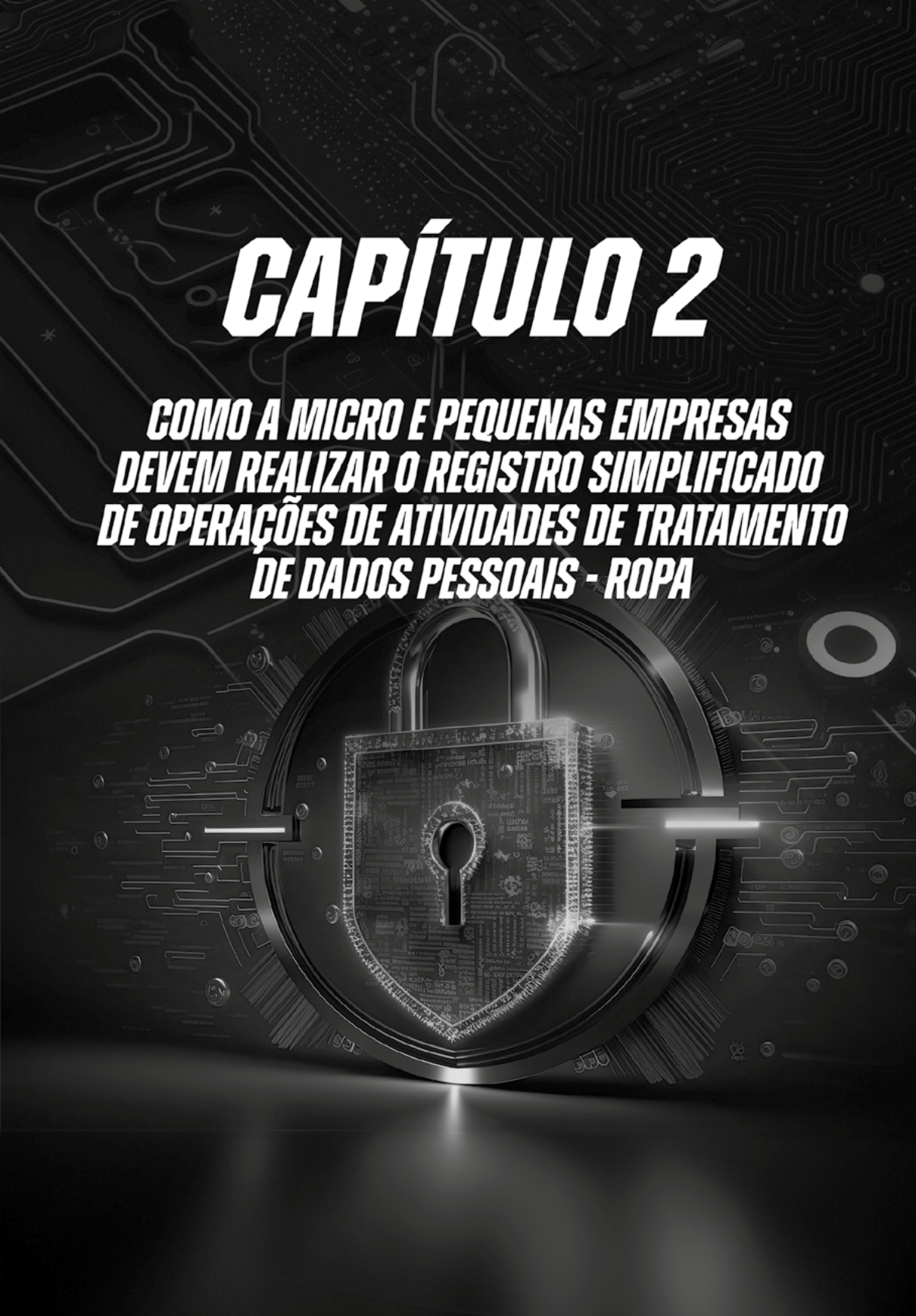
SILVA, Antônio Everardo Nunes da. Segurança da Informação. Rio de Janeiro: Ciência Moderna, 2012.

SILVEIRA, Sergio Amadeu. "Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais". Liinc em Revista, São Paulo: Edições Sesc São Paulo, 2017.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016.

CAPÍTULO 2

COMO A MICRO E PEQUENAS EMPRESAS DEVEM REALIZAR O REGISTRO SIMPLIFICADO DE OPERAÇÕES DE ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS - ROPA



Poliane Almeida Silva Dias[4]

RESUMO: O Registro Simplificado de Operações de Tratamento de Dados Pessoais – ROPA, é uma ferramenta essencial para garantir a conformidade com a regulamentação de proteção de dados, a Lei Geral de Proteção de Dados Pessoais (LGPD) [5] no Brasil. Esse registro é um documento detalhado que descreve todas as atividades relacionadas ao processamento de dados pessoais realizadas por uma organização. Neste artigo, iremos trazer uma abordagem prática e visual de como a Micro e Pequenas Empresas poderão implementar o ROPA de modo a atender aos parâmetros legais da conformidade, visando à proteção dos direitos fundamentais de privacidade do titular de dados no Brasil.

PALAVRAS-CHAVE: LGPD – ROPA – Ferramentas – Conformidade – Micro e Pequenas Empresas

ABSTRACT: The Simplified Registration of Personal Data Processing Operations – ROPA, is an essential tool to ensure compliance with data protection regulations, the General Personal Data Protection Law (LGPD) in Brazil. This record is a detailed document that describes all activities related to the processing of personal data carried out by an organization. In this article, we will bring a practical and visual approach to how Micro and Small Companies can implement ROPA to meet the legal parameters of compliance, aiming to protect the fundamental privacy rights of the data subject in Brazil.

---

4 Poliane Almeida Silva Dias: Advogada e bacharel em Direito pela PUC/MG, Palestrante e Analista Sênior em Privacidade/Proteção de Dados. Pós-graduada em Direito Civil pela PUC/MG e Pós-graduada em Direito Digital e Proteção de Dados pela Ebradi. Com certificações internacionais em Privacidade e Proteção de Dados (CIPM e CDPO/BR) pela IAPP - (International Association of Privacy Professionals). Presidente da Comissão de Proteção de Dados da OAB/MG Subseção de Betim, Membro da Comissão de Proteção de Dados da OAB/MG e Membro da Comissão Internacional de Proteção de Dados da ABA – Associação Brasileira de Advogados. @polianealmeida.adv

5 BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 14 abr. 2024.

KEYWORDS: LGPD – ROPA – *Tools – Compliance – Micro and Small Businesses*

1. INTRODUÇÃO

O Registro Simplificado de Operações de Tratamento de Dados Pessoais – ROPA - é uma peça fundamental no universo da proteção de dados e privacidade aos Agentes de Tratamento de Pequeno Porte (ATPP). Em um mundo cada vez mais digitalizado, em que informações pessoais são constantemente coletadas, armazenadas e processadas, é essencial que as organizações adotem práticas transparentes e responsáveis para garantir a segurança e privacidade desses dados.

O Registro de Atividades entra em cena como uma ferramenta que visa documentar e detalhar todas as operações relacionadas ao tratamento de dados pessoais realizadas por uma empresa ou entidade. Desde a coleta até o descarte, passando pelo armazenamento, compartilhamento e eventual transferência, esse registro oferece uma visão abrangente e transparente das atividades de processamento de dados, proporcionando não apenas conformidade legal, mas também transparência e confiança aos titulares dos dados.

Neste artigo, exploraremos a importância do Registro Simplificado de Operações de Tratamento de Dados Pessoais - ROPA, seus objetivos, componentes essenciais e seu papel na conformidade com as regulamentações de proteção de dados em vigor.

Além de esclarecer o que compõe esse registro simplificado, tais como: dados pessoais, dados pessoais sensíveis, bases legais e medidas de segurança para proteção das informações pessoais.

2. O QUE SÃO DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

O artigo 5º da LGPD[6] traz que dado pessoal é informação relacionada à pessoa natural identificada ou identificável.

O autor Rony Vainzof (2019)[7] esclarece que "dado pessoal, pelo qual não somente a informação relativa à pessoa diretamente identificada estará protegida pela Lei, mas também aquela informação que possa – tem o potencial de – tornar a pessoa identificável".

Ainda segundo o autor, nome, prenome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, gênero, profissão, origem social e ética: informações relativas à saúde, à genética, à orientação sexual, às convicções políticas, religiosas e filosóficas: números de telefone, registros de ligações, protocolos de internet, registros de conexão, registros de acesso a aplicações de internet, contas de e-mail, cookies, hábitos, gostos e interesses, são apenas alguns exemplos de dados pessoais que pautam a atual vida em sociedade.

Portanto, o objetivo central da LGPD não é a proteção a qualquer dado, e sim aqueles dados intrinsecamente vinculados a uma pessoa natural identificada ou identificável.

Podemos classificar os dados, de acordo com a LGPD, da seguinte forma, como apontada pelo autor Rony Vainzof[8] (2019):

6 BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 20 abr. 2024.

7 LGPD. Lei Geral de Proteção de Dados comentada / coordenadores Viviane Nóbrega Maldonado e Renato Pice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, pág 89, 2019.

8 LGPD. Lei Geral de Proteção de Dados comentada / coordenadores Viviane Nóbrega Maldonado e Renato Pice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, pág. 91, 2019.

- **Dados pessoais diretos:** identifica diretamente uma pessoa natural, sem a necessidade de outras informações, como CPF, RG, título de eleitor, nome (se não houver homônimos);
- **Dados pessoais indiretos:** torna a pessoa natural identificável, pois necessitam de informações adicionais para identificá-la, como gostos, interesses, hábitos de consumo, profissão, sexo, idade e geolocalização;
- **Dados pessoais pseudonimizados:** dado que perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;
- **Dado anonimizado, que não são dados pessoais:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Já os dados pessoais sensíveis são informações pessoais que possam trazer algum tipo de discriminação quando do seu tratamento (origem racial, convicção religiosa, opinião política, dado referente à saúde, dados genéticos e biométricos. Ou seja, são dados pessoais que poderão implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares, conforme descrito pelo autor Rony Vainzof (2019) [9].

Segundo o autor, a LGPD consegue dedicar obrigações diferenciadas ao tratamento de dados sensíveis:

- As bases legais (ver tópico abaixo) para tratamento de dados pessoais sensíveis são diferenciadas e limitadas, dispostas no art. 11, da LGPD;

9 LGPD. Lei Geral de Proteção de Dados comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, pág 92 e 93, 2019.

- Quando a base legal para o tratamento for o consentimento, além de ser livre, inequívoco e informado, também deverá ser específico e destacado;
- Não há base legal para o tratamento de dados sensíveis por interesse legítimo;
- Não há base legal para o tratamento de dados sensíveis por proteção do crédito. Inclusive, a Lei do Cadastro Positivo veda, expressamente, anotações de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas";
- Da mesma forma, não há base legal para tratamento de dado sensível para a execução de contrato ou procedimentos preliminares relacionados a contrato, mas, sim, para o exercício regular de diretos, inclusive em contrato;
- Há base legal específica quando o tratamento de dado sensível servir para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos;
- A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores, com o objetivo de obter vantagem econômica, poderá ser objeto de vedação ou de regulamentação por parte da ANPD, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências;
- É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, exceto nas hipóteses de portabilidade de dados quando consentido pelo titular ou necessidade de comunicação para a adequada prestação de serviços de saúde suplementar.

3. BASES LEGAIS AUTORIZADORAS DO TRATAMENTO DE DADOS PESSOAIS

Na LGPD, as bases legais[10] descritas no artigo 7º, trazem os fundamentos que permitem o tratamento de dados pessoais de acordo com a Lei. São condições específicas nas quais uma organização pode coletar, armazenar, usar ou compartilhar dados pessoais de indivíduos. As bases legais fornecem uma justificativa para o processamento de dados e garantem que esse processamento seja feito de maneira legal e ética.

As bases legais estabelecidas pela LGPD são:

- **Consentimento:** O tratamento de dados pessoais é permitido quando o titular dos dados dá consentimento específico para uma finalidade determinada;
- **Execução de Contrato:** O tratamento é necessário para a execução de um contrato do qual o titular dos dados faz parte, ou para medidas preliminares relacionadas a um contrato;
- **Cumprimento de obrigação legal ou regulatória:** O tratamento é necessário para o cumprimento de uma obrigação legal ou regulatória pelo controlador;
- **Proteção da vida ou da incolumidade física do titular ou terceiros:** O tratamento é necessário para proteger a vida ou a integridade física do titular dos dados ou de terceiros;
- **Interesse Legítimo:** O tratamento é necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto nos casos em que interesses ou direitos e liberdades fundamentais do titular dos dados exijam a proteção de dados pessoais e se sobreponham a esses interesses legítimos;
- **Tutela da saúde:** O tratamento é necessário para a tutela da saúde, exclusivamente, em procedimento realizado por

10 BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 20 abr. 2024.

profissionais de saúde, serviços de saúde ou autoridade sanitária;

- **Interesse Público:** O tratamento é necessário para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- **Proteção do crédito:** O tratamento é necessário para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

É importante ressaltar que o tratamento de dados pessoais deve sempre observar os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção de danos, não discriminação e responsabilização e prestação de contas, conforme estabelecido pela LGPD.

4. MEDIDAS DE SEGURANÇA TÉCNICA PARA A MICRO E PEQUENAS EMPRESAS

O Guia Orientativo "Segurança da Informação para Agentes de Tratamento de Pequeno Porte"[11] foi lançado pela ANPD para auxiliar micro e pequenas empresas na implementação de medidas de segurança da informação de acordDo com a LGPD.

Algumas das medidas descritas neste guia são:

- **Política de Segurança da Informação (PSI):** Desenvolvimento e implementação de uma PSI que estabeleça diretrizes para proteger os dados pessoais e promova a conscientização sobre segurança da informação entre os colaboradores;
- **Controle de acesso:** Implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso

11 GOV BR. ANPD. Segurança da Informação para Agentes de tratamento de Pequeno Porte. Disponível em https://www.gov.br/anpd/pt-br/documentos-e- publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf Acesso em: 20 abr. 2024.

aos dados pessoais, utilizando métodos como senhas fortes, autenticação de dois fatores e restrição de acesso por perfil;

- **Gestão de dispositivos e ativos:** Manutenção de um inventário de dispositivos e ativos de informação, bem como implementação de políticas de segurança para proteger esses dispositivos contra ameaças internas e externas;
- **Gestão de incidentes de Segurança da Informação:** Estabelecimento de procedimentos para detectar, responder e recuperar-se de incidentes de segurança da informação, incluindo a criação de um plano de resposta a incidentes;
- **Monitoramento de Ambiente de TI:** Implementação de sistemas de monitoramento para identificar e responder a atividades suspeitas nos ambientes de TI da empresa, como tentativas de acesso não autorizado ou comportamento anômalo;
- **Backup e Recuperação de dados:** Realização de backups regulares dos dados e implementação de procedimentos de recuperação para garantir a disponibilidade e a integridade dos dados em caso de incidentes;
- **Gestão de Fornecedores e contratados:** Avaliação da segurança da informação de fornecedores e contratados que tenham acesso aos dados pessoais da empresa, por meio de cláusulas contratuais e monitoramento adequado;
- **Conscientização e treinamento:** Realização de treinamentos regulares para funcionários sobre segurança da informação, abordando temas como reconhecimento de ameaças, procedimentos de segurança e políticas da empresa.

Essas são algumas das medidas destacadas no guia da ANPD, que visa orientar as Micros e Pequenas Empresas na proteção dos dados pessoais conforme exigido pela LGPD. É importante que as empresas adaptem essas medidas de acordo com suas necessidades específicas e recursos disponíveis.

5. O QUE A ANPD REGULAMENTOU SOBRE O REGISTRO SIMPLIFICADO DE OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS – ROPA

A ANPD – Autoridade Nacional de Proteção de Dados publicou, em 27 de janeiro de 2022, o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte (ATPP). [12]

Com isso, a ANPD determinou que haveria um regramento específico sobre o Registro de Operações de tratamento de dados pessoais, em seu artigo 9º:

> [...]" **Seção II**
> **Do Registro das Atividades de Tratamento**
> **Art. 9º** Os agentes de tratamento de pequeno porte podem cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do art. 37 da LGPD, de forma simplificada.
> **Parágrafo único.** A ANPD fornecerá modelo para o registro simplificado de que trata o caput.

Portanto, em 14 de junho de 2023, a Autoridade Nacional de Proteção de Dados divulgou o modelo de Registro Simplificado de Operações com dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP) [13].

12 GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº 2, de 27 de janeiro de 2002. Imprensa Nacional. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper . Acesso em: 14 abr. 2024.

13 GOV BR. Ministério da Justiça e Segurança Nacional. ANPD divulga modelo de registro simplificado de operações com dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP). Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-modelo-de-registro-simplificado-de-operacoes-com-dados-pessoais-para-agentes-de-tratamento-de-pequeno-porte-atpp . Acesso em: 14 abr. 2024.

O modelo proposto apresenta uma estrutura simplificada de registro de atividades de tratamento de dados pessoais, adequada às necessidades e recursos limitados da Micro e Pequenas Empresas.

O Registro Simplificado inclui seções para registrar informações essenciais sobre as operações de processamento de dados realizadas pela organização, tais como:

a. **Informações de contato:** nome da organização, CNPJ, endereço, principal atividade, gestor responsável, e-mail, telefone e data do registro;
b. **Categorias de titulares:** com opções de marcações para titulares em geral, crianças e adolescentes e idosos;
c. **Dados pessoais:** nome, endereço, RG, CPF, e-mail, telefone e outros;
d. **Medidas de segurança:** Listar medidas de segurança utilizadas para proteção dos dados pessoais. Ex.: controle de acesso, antivírus atualizado, backups, pseudonimização, firewall, etc.
e. **Período de armazenamento:** a organização deverá informar qual o prazo de retenção dos dados pessoais dentro do processo de tratamento;
f. **Processo, finalidade e hipótese legal:** Informar o nome do processo interno ao qual o presente registro se refere (tratamento de dados realizado), a finalidade (motivo do tratamento) e a hipótese legal que justifica o tratamento realizado, conforme os artigos 7º e 11 da LGPD;
g. **Compartilhamento:** Descrever o fluxo de compartilhamento para fora da organização e o nome dos terceiros com quem os dados foram compartilhados;
h. **Observações:** Inserir informações opcionais, se houver, como dados de encarregados e de operadores, e sobre transferências internacionais de dados pessoais, se for o caso, etc.

6. INTERNAMENTE, QUEM DEVERÁ REALIZAR O REGISTRO SIMPLIFICADO DE OPERAÇÕES

O registro simplificado de operações de tratamento de dados pessoais geralmente é realizado pelo departamento de conformidade ou pelo departamento responsável pela proteção de dados dentro de uma organização, quando essas empresas não possuem o seu Encarregado de Dados, haja vista a dispensa da contratação desse profissional.

Em algumas empresas de menor porte, esse registro pode ser feito pelo próprio responsável pelo tratamento de dados, especialmente se não houver um departamento específico para essa finalidade.

O importante é que a responsabilidade pela documentação das atividades de tratamento de dados seja atribuída a uma área que compreenda os requisitos legais de proteção de dados e tenha conhecimento das práticas internas de processamento de dados da organização.

7. COMO ESTRUTURAR AS ESTREVISTAS DE MAPEAMENTO DE DADOS PESSOAIS EM CADA DEPARTAMENTO INTERNO

Para estruturar as entrevistas de mapeamento de dados pessoais em cada departamento interno de uma organização, é importante seguir um processo bem definido e abordar diferentes aspectos relacionados ao tratamento de dados. Aqui está uma sugestão de como estruturar essas entrevistas:

a) Preparação:

- Identifique os principais departamentos ou áreas da organização que lidam com o processamento de dados pessoais;

- Agende reuniões com os responsáveis de cada departamento para discutir o mapeamento de dados pessoais;
- Prepare um roteiro de entrevista que aborde os principais pontos relacionados ao tratamento de dados pessoais, com base no modelo simplificado descrito no capítulo 3 deste artigo.

b) Abordagem inicial:

- Explique o propósito das entrevistas de mapeamento e a importância de compreender como os dados pessoais são coletados, quais dados pessoais são necessários, se existem dados sensíveis no processo, se foram coletados dados de crianças e adolescentes, com quais departamentos esses dados são compartilhados internamente (e a finalidade desses compartilhamentos), como são armazenados, se há o compartilhamento com terceiros e qual o prazo de retenção dos dados;
- Estabeleça confiança e demonstre que o objetivo é ajudar na conformidade com as regulamentações de proteção de dados e na proteção dos direitos dos titulares dos dados. Caso contrário, o entrevistado sentirá que está sendo fiscalizado e poderá não cooperar.

c) Roteiro de entrevista:

- Identificação de dados pessoais: Peça aos entrevistados que descrevam os tipos de dados pessoais que são coletados e utilizados em suas atividades e em cada processo;
- Finalidade do processamento: Questione sobre as razões pelas quais os dados são coletados e como são utilizados em cada departamento;

- Base legal para o processamento: Verifique se existe uma base legal adequada para o processamento dos dados pessoais em conformidade com a legislação aplicável;
- Compartilhamento de dados: Explore, se, e como os dados pessoais são compartilhados dentro e fora do departamento;
- Medidas de segurança: Pergunte sobre as medidas de segurança adotadas para proteger os dados pessoais contra acesso não autorizado, uso indevido ou divulgação;
- Retenção e descarte de dados: Descubra por quanto tempo os dados pessoais são retidos e como são descartados quando não são mais necessários.

d) Documentação:

- Registre todas as informações coletadas durante as entrevistas de mapeamento de dados pessoais;
- Compile um relatório que destaque os principais pontos identificados em cada departamento, incluindo os tipos de dados pessoais coletados, finalidades de processamento, bases legais, medidas de segurança e procedimentos de retenção e descarte. Para isso, utilize o modelo simplificado disponibilizado pela ANPD.

c) Análise e ações subsequentes:

- Analise os resultados do mapeamento para identificar áreas de risco, lacunas de conformidade ou oportunidades de melhoria;
- Desenvolva um plano de ação para abordar quaisquer problemas identificados e implementar medidas corretivas ou preventivas, conforme necessário.

Ao seguir esta estrutura, as entrevistas de mapeamento de dados pessoais em cada departamento interno podem fornecer uma visão

abrangente das práticas de tratamento de dados da organização e ajudar na implementação eficaz de medidas de proteção de dados e conformidade regulatória.

8. ROPA EM LEGAL DESIGN: ABORDAGEM DO REGISTRO DE OPERAÇÕES DE TRATAMENTO MAIS VISUAL

Após um período de estudos e levantamentos dos pontos imprescindíveis do Registro de Operações, o querido colega e profissional Guilherme Gonçalves Pereira, e esta autora que vos fala, desenvolvemos um ROPA mais visual.

Elaborado com técnicas do Legal Design, o material visa melhorar a conscientização sobre o tema e auxiliar o processo de implementação de agentes de tratamento da Micro e Pequenas Empresas.

O documento denota algo mais didático e de fácil entendimento, que não substitui o modelo proposto pela ANPD, mas que auxilia visualmente sobre um tema complexo.

O documento é de livre consulta e uso, e poderá ser acesso no link abaixo em nota de rodapé[14].

14 ROPA EM LEGAL DESIGN. Autores Poliane Almeida Silva Dias e Guilherme Gonçalves Pereira. Publicado em 1 de dezembro de 2022 nas redes sociais de ambos os autores. Disponível em https://drive.google.com/drive/u/2/folders/1vR_szJXlABLwkTQpRBJgRYa4mdk4L6RJ . Acesso em: 14 abr. 2024.


Origem dos dados:
REGISTRO DE OPERAÇÕES
DATA VERSÃO DISP.: __/__/____
SETOR: _____
CATEGORIA DO TITULAR: _____
RESPONSÁVEL INTERNO: _____
ATIVIDADE DE NEGÓCIO – PROCESSO:
FINALIDADE DA COLETA:
QUAIS OS DADOS PESSOAIS:
RISCOS ENCONTRADOS:
CONTATOS DOS AGENTES ENVOLVIDOS:
LOCAL DE ARMAZENAMENTO (FÍSICO E DIGITAL):
HAVERÁ O COMPARTILHAMENTO COM TERCEIROS? QUAIS?
CATEGORIA DOS DADOS:
TRANSFERÊNCIA INTERNACIONAL:
Sim
Não
Para quais países:
MEDIDAS DE SEGURANÇA:
-
RECOMENDAÇÕES:
-
PRECISA ELABORAR RIPD?
POSIÇÃO COMO AGENTE DE TRATAMENTO:
BASE LEGAL:
LEIS APLICÁVEIS:
ENCARREGADO DE DADOS / CONTATO:
PERÍODO DE RETENÇÃO:
RESERVADO OS DIREITOS AUTORAIS. LIVRE PARA USO SEM RETIRAR OS NOMES DOS AUTORES: ADV. GUILHERME GONÇALVES E ADV. POLIANE ALMEIDA.

Fonte: Material e arte desenvolvidos pelos profissionais Guilherme Gonçalves Pereira e Poliane Almeida Silva Dias

Nota-se que o modelo, em Visual Law acima, traz alguns pontos extras e diferentes do modelo proposto pela ANPD, mas, na essência, são comuns e descrevem quais informações são necessárias durante o mapeamento de dados pessoais (entrevistas a serem realizadas com os responsáveis pelos departamentos).

11. CONCLUSÃO

Em conclusão, o Registro Simplificado de Operações de Tratamento de Dados Pessoais (ROPA) é uma ferramenta vital para garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Este documento detalhado descreve todas as atividades relacionadas ao processamento de dados pessoais realizadas por uma organização, proporcionando transparência, responsabilidade e confiança aos titulares dos dados.

A Autoridade Nacional de Proteção de Dados (ANPD) estabeleceu diretrizes específicas para agentes de tratamento de pequeno porte (ATPP), permitindo um registro simplificado das operações de tratamento de dados. Esse modelo simplificado fornece uma estrutura clara e acessível para Micro e Pequenas Empresas, ajudando-as a cumprir suas obrigações legais de forma eficiente.

No que diz respeito à implementação interna, o registro simplificado geralmente é conduzido pelo departamento de conformidade ou pela equipe responsável pela proteção de dados dentro da organização. Em empresas menores, o próprio responsável pelo tratamento de dados pode realizar esse registro, desde que compreenda os requisitos legais e tenha conhecimento das práticas internas de processamento de dados.

Em última análise, o Registro Simplificado de Operações de Tratamento de Dados Pessoais desempenha um papel crucial na proteção dos direitos fundamentais de privacidade dos indivíduos, promovendo uma cultura de responsabilidade e transparência no tratamento de dados pessoais em conformidade com a legislação de proteção de dados em vigor.

REFERÊNCIAS

BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 abril. 2024.

CHAT GPT. Plataforma de Pesquisa com a utilização da Inteligência Artificial. Disponível em https://chat.openai.com. Acesso em 05 abril.2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº 2, de 27 de janeiro de 2002. Imprensa Nacional. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper . Acesso em: 14 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. ANPD divulga modelo de registro simplificado de operações com dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP). Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-modelo-de-registro-simplificado-de-operacoes-com-dados-pessoais-para-agentes-de-tratamento-de-pequeno-porte-atpp . Acesso em: 14 abr. 2024.

GOV BR. ANPD. Segurança da Informação para Agentes de tratamento de Pequeno Porte. Disponível em https://www.gov.br/anpd/pt-br/documentos-e- publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf Acesso em: 20 abr. 2024.

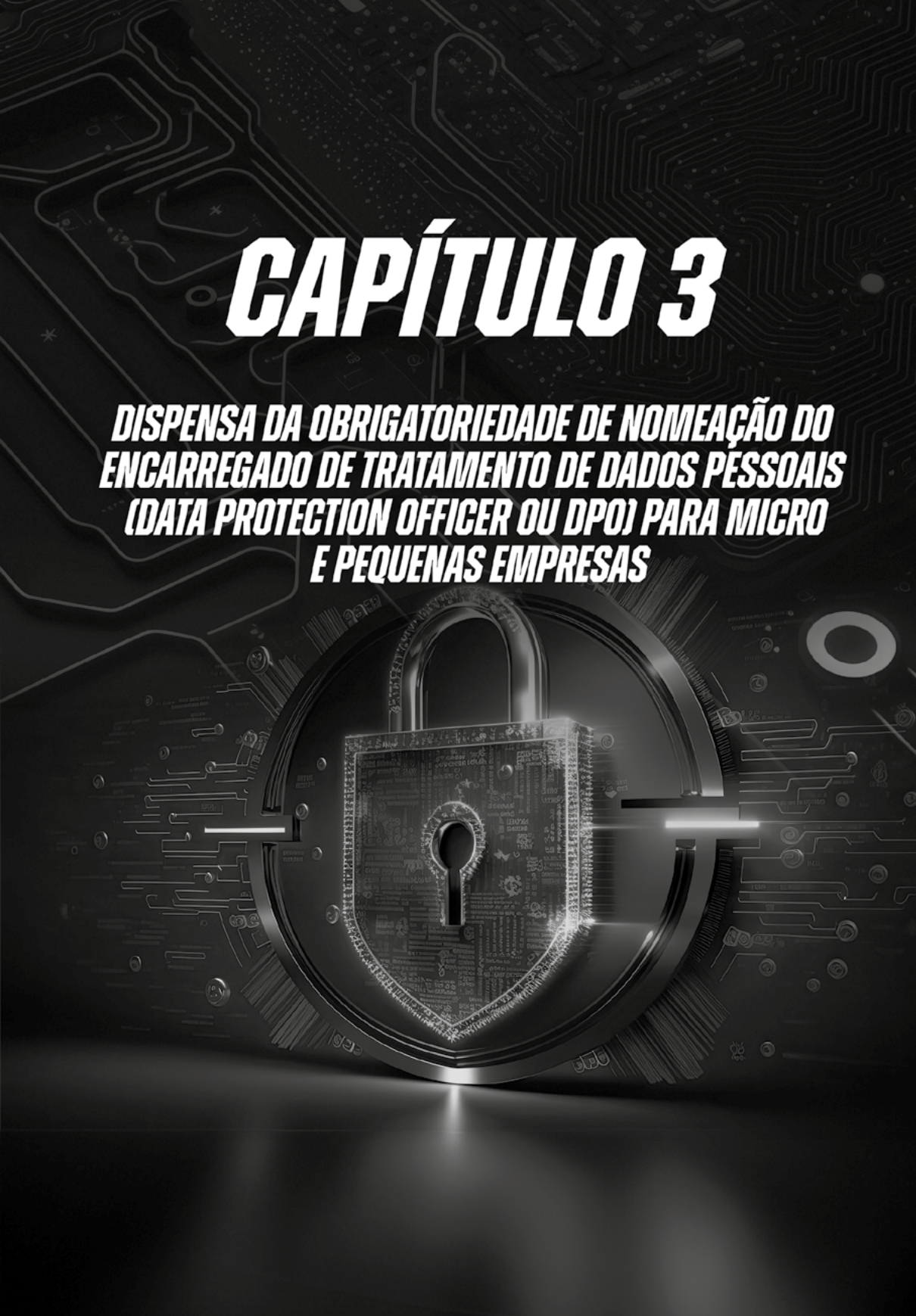
LGPD. Lei Geral de Proteção de Dados comentada / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019.

ROPA EM LEGAL DESIGN. Autores Poliane Almeida Silva Dias e Guilherme Gonçalves Pereira. Publicado em 01 de dezembro de 2022

nas redes sociais de ambos os autores. Disponível em https://drive.google.com/drive/u/2/folders/1vR_szJXlABLwkTQpRBJgRYa4mdk4L-6RJ . Acesso em: 14 abr. 2024.

CAPÍTULO 3

DISPENSA DA OBRIGATORIEDADE DE NOMEAÇÃO DO ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS (DATA PROTECTION OFFICER OU DPO) PARA MICRO E PEQUENAS EMPRESAS



Pauliana Roberta Mota de Abreu[15]

RESUMO: A Autoridade Nacional de Proteção de Dados – ANPD - oportunizou aos agentes de tratamento de pequeno porte medidas mais brandas no que se refere ao tratamento de dados pessoais. Isto é, trouxe flexibilização quanto a alguns temas contidos na Lei Geral de Proteção de Dados, os quais para estas pequenas empresas eram empecilhos à adequação de fato da norma. Para tanto, restou promulgada a Resolução CD/ANPD nº 2, de 27 janeiro de 2022. Neste artigo, veremos em especial um dos assuntos mitigados pela resolução: a flexibilização quanto a dispensa da obrigatoriedade de nomeação do Encarregado/Data Protection Officer (DPO) para agentes de tratamento de pequeno porte, sem que houvesse, portanto, prejuízo aos titulares de dados pessoais. Acontece que dentro desta mitigação trazida pela lei é possível verificar que nem todas as micro e pequenas empresas estão desobrigadas a constituir o cargo de Encarregado de tratamento de dados pessoais, tamanha é a importância dessa figura ante os agentes de tratamento de dados e os titulares de dados pessoais. E, ainda que exista a dispensa da obrigação do Encarregado, Data Protection Officer (DPO), a lei não retira dos agentes de tratamento de pequeno porte suas responsabilidades junto ao titular de dados, estando estes obrigados a manter um canal de comunicação entre a empresa e o titular de dados pessoais. Contudo, fica a cargo da empresa de pequeno e médio porte aderir ou não o Encarregado em sua estrutura organizacional.

PALAVRAS-CHAVES: Pequenas e médias empresas. Flexibilização. Encarregado de Tratamento de Dados.

ABSTRACT: The National Data Protection Authority – ANPD, provided small processing agents with more lenient measures regarding the processing of personal data. That is, it brought flexibility regarding

15 Pauliana Roberta Mota de Abreu, graduada em Direito pela PUC Minas; Pós-graduada em Direito e Processo do Trabalho, e em Docência e Marketing Jurídico com especialização em Educação, Tecnologia e Empreendedorismo; Advogada Civilista há mais de 10 (dez) anos; atuante na comissão Direito Na Escola, como Vice-Presidente; e como membro na Comissão Proteção de Dados Pessoais, ambas as Comissões da OAB/MG Subseção Betim/MG.

some topics contained in the General Data Protection Law, which for these small companies were obstacles to the actual adaptation of the standard. To this end, CD/ANPD Resolution n.º. 2, dated January 27, 2022, was promulgated. In this article, we will look at one of the issues mitigated by the resolution: the flexibility regarding the exemption from the mandatory appointment of the Data Protection Officer (DPO) for small processing agents, without, therefore, causing harm to the holders of personal data. It turns out that within this mitigation brought by the law, it is possible to verify that not all micro and small companies are exempt from establishing the position of person in charge of processing personal data, such is the importance of this figure in relation to data processing agents and data holders. personal data. And, even though there is an exemption from the obligation of the person in charge, Data Protection Officer (DPO), the law does not remove from small processing agents their responsibilities towards the data subject, as they are obliged to maintain a communication channel between the company and the holder of personal data. However, it is up to the small and medium-sized company whether to accept the person in charge in its organizational structure.

KEYWORDS: Small and medium-sized companies. Flexibilization. Data Processing Officer.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais - LGPD[16] - foi criada a fim de direcionar o manuseio de dados pessoais em geral pelos gestores de instituições e órgãos públicos e privados e garantir aos usuários segurança quanto aos seus dados a eles expostos. As normas contidas nesta Lei se movimentam no sentindo de trazer as diretrizes para a adequação desses agentes de tratamento de dados, como também na imposição de sanções pelo descumprimento de suas regras.

16 BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/l13709.htm. Acesso em: 14 abril. 2024.

Entretanto, como toda Lei que mesmo após sua promulgação se adapta às necessidades do seu público-alvo, não foi diferente com a Lei de Proteção de Dados Pessoais, que se viu obrigada a se moldar em alguns pontos a realidade que a prática exigiu.

Assim, em específico para as pequenas e médias empresas, que é o foco do nosso estudo, a LGPD em seu artigo 41, §3º, deixou em aberto a possibilidade de a Autoridade Nacional de Proteção de Dados determinar normas complementares quanto à dispensa da indicação do Encarregado pelo tratamento de dados pessoais.

Neste cenário, surge a Resolução CD/ANPD nº 2, de 27 janeiro de 2022[17], que trouxe algumas mudanças no dispositivo da Lei Geral de Proteção de Dados Pessoais inclusive quanto à flexibilização das obrigações dos agentes de tratamento de pequeno porte no cumprimento da alusiva norma.

Contudo, o que veremos a seguir trata especificamente da dispensa da obrigatoriedade de nomeação do Encarregado (*Data Protection Officer* ou DPO) para determinadas micros e pequenas empresas, porém, não como uma verdade absoluta, visto que há previsão naquela Resolução de se manter um canal de comunicação para que os clientes possam exercer seus direitos em face dos seus dados pessoais junto àquele agente de tratamento.

E, para tanto, faz-se forçoso trazermos a definição de Encarregado ou *Data Protection Officer* (DPO) e o seu significado no mundo da proteção de dados, para que possamos entender que a sua dispensa para as pequenas e médias empresas não acarreta prejuízo aos envolvidos (controlador, encarregado, operador e titular), se for implementado, de fato, um canal para o agente de tratamento de pequeno porte dentro, é claro, das diretrizes da Lei Geral de Proteção de Dados Pessoais e a Autoridade Nacional de Proteção de Dados - ANPD.

17 GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº 2, de 27 de janeiro de 2002. Imprensa Nacional. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper . Acesso em: 14 abr. 2024.

No entanto, a aderência da figura do Encarregado de Dados (DPO) dentro da empresa ou organização, independentemente de seu tamanho, finalidade ou natureza, acarreta um diferencial enorme no tráfico dos negócios, tanto para a própria empresa ou organização quanto para os clientes (titulares de dados pessoais).

2. FLEXIBILIZAÇÃO DA LGPD AOS MICROS E PEQUENAS EMPRESAS

A Resolução CD/ANPD nº 2, de 27 janeiro de 2022, regula a aplicação da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018) para agentes de tratamento de pequeno porte, não se aplicando, portanto, ao tratamento de dados pessoais realizados por pessoas naturais para fins exclusivamente particulares, e não econômicos.

A Resolução tem como propósito facilitar a adaptação e adequação de agentes de tratamento de pequeno porte às normas da Lei Geral de Proteção de Dados, a fim de evitar custos e, conforme o caso, prazos desproporcionais às atividades desses agentes.

Entre outras determinações, esta norma trouxe a flexibilização com base no risco e escala do tratamento de dados pessoais, quer sejam: a flexibilização do atendimento às requisições dos titulares por meio eletrônico ou impresso; a dispensa da obrigação de eliminar, anonimizar ou bloquear dados excessivos; o dobro do prazo com relação a outros agentes de tratamento; a flexibilização do relatório de impacto como forma simplificada; e, por fim, a dispensa da obrigação de nomear um DPO/Encarregado de tratamento de dados pessoais. Sendo esta última determinação a que abordaremos neste artigo.

3. OS AGENTES DE TRATAMENTO DE PEQUENO PORTE

Pois bem. Para melhor entendimento, importante trazermos o que para a Resolução CD/ANPD nº 2, de 27 janeiro de 2022, são os agentes de tratamento de pequeno porte, assim definidos como: microempresas, empresas de pequeno porte, startups, pessoas

jurídicas de direito privado, inclusive sem fins lucrativos, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

Porém, a referida Resolução, em seu artigo 3º, é bastante enfática quando afirma que nem todos os agentes de tratamento de pequeno porte poderão se beneficiar da condição jurídica ali diferenciada.

Os agentes de tratamento de pequeno porte que fazem parte da exceção à regra são: os que realizam tratamento de alto risco para os titulares; os que aufiram receita bruta superior por ano de R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais); ou os que pertençam a grupo econômico de fato ou de direito, cuja receita global ultrapasse os limites referidos no inciso II, conforme o caso.

Assim, este artigo é principalmente para aqueles agentes de tratamento de pequeno porte que se enquadram nas diretrizes da Resolução CD/ANPD nº 2, de 27 janeiro de 2022, com ênfase no que diz respeito à dispensa da obrigatoriedade de nomeação do Encarregado/ *Data Protection Officer* (DPO).

Desta feita, se você está em alguma ou algumas das definições descritas acima, este artigo pode ajudar sua empresa ou organização a funcionar conforme os ditames da norma de proteção de dados, e, assim, garantir aos seus usuários a proteção necessária e exigida por lei.

Entretanto, vale lembrar que as pequenas e médias empresas não estão isentas de realizar a adequação à Lei Geral de Proteção de Dados Pessoais, tão somente, terão em alguns casos tratamento diferenciado. Pois, em que pese a especificidade destas empresas em muitos aspectos, há de se respeitar em primeiro lugar o direito fundamental do titular de dados em face da proteção que lhe é devida aos seus dados pessoais, observando a boa-fé e aos princípios da lei, tais como: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

A esse respeito, a Resolução CD/ANPD 2/22, em seu artigo 16, estabelece que a Autoridade Nacional de Proteção de Dados poderá determinar ao agente de tratamento de pequeno porte o cumprimento das obrigações dispensadas ou flexibilizadas pela norma, considerando determinadas conjunturas, como a natureza ou o volume das operações, assim como os riscos para os titulares.

4. MAS, POR QUE OFERECER TRATAMENTO DISTINTO ÀS EMPRESAS MÉDIAS E DE PEQUENO PORTE?

De acordo com o portal do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas – SEBRAE[18], a rigidez da Lei Geral de Proteção de Dados Pessoais seria um obstáculo para as empresas pequenas e de médio porte executarem com as suas determinações, gerando a elas diversos processos e possíveis multas em desfavor destas empresas. Assim, a flexibilização para os "pequenos negócios" surge para facilitar o cumprimento das determinações advindas da Lei, difíceis de serem executadas.

Ainda pelo entendimento do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas – SEBRAE, a baixa maturidade e a falta de uma cultura de proteção de dados pessoais pelas empresas de pequeno porte poderiam dificultar a adequação à Lei Geral de Proteção de Dados Pessoais e inviabilizar sua existência.

Isso porque a LGPD é uma legislação um tanto ou quanto complexa a ser adotada, sendo certo que, para estar em sua conformidade, não basta elaborar um projeto de adequação à Lei, mas efetivamente implementar uma gestão hábil do programa de privacidade e de proteção de dados, e, assim, atingir os objetivos exigidos na norma.

Um fato interessante é que, quando não se alcança os propósitos da Lei, temos a probabilidade do risco se materializar gerando sequelas

18 SEBRAE. LGPD: qual o impacto nos pequenos negócios? Sua pequena empresa está preparada. Disponível em https://www.sebrae-sc.com.br/blog/lgpd-qual-o-impacto-nos-pequenos-negocios-sua-pequena-empresa-esta-preparada Acesso em: 15 abr. 2024.

para os envolvidos. O risco, na percepção de *Tiago Neves Furtado*[19], é a possibilidade de perigo ou ameaça, ou como a probabilidade de prejuízo ou insucesso que gera consequências tanto para o titular dos dados tradados quanto para a organização ou empresa que gere esses dados.

As consequências da concretização do risco aos titulares de dados podem ser diversas, apresentando-se, entre outros, como um mero aborrecimento, perdas financeiras e até mesmo abalos psicológicos. Ao passo que, para os agentes de tratamento de dados pessoais, as implicações consistem em multas, advertência, publicização da infração, bloqueio ou eliminação de dados pessoais. Sem contar na consequência reputacional, que, em que pese não estar prevista na lei, é ditada culturalmente pela sociedade. (Artigo 52, LGPD)

Para Tiago, "*Tratar dados pessoais é gerir risco a todo momento. É entender qual a consequência (impacto) de não se cumprir algum objetivo (probabilidade) da LGPD.*"

Importante levantar a questão de que a Lei de Proteção de Dados Pessoais brasileira, quando voltada para o fato punitivo, baseia-se, conforme a Resolução CD/ANPD n. 1/2021, na lógica do risco verificado no processo fiscalizatório, fazendo distinção de gravidade de acordo com a natureza das sanções.

Portanto, por tudo que já vimos até agora, digo que há caminhos diferentes que alcançam o mesmo fim, que é proteger o tratamento de dados a partir do seu titular, sem que haja consequências danosas às empresas de pequeno porte, tão severas.

Neste sentido, atendendo às duas partes principais envolvidas neste cenário (o titular de dados pessoais e o agente de tratamento desses dados), em especial as pequenas e médias empresas, houve a mitigação da norma (LGPD) com a Resolução CD/ANPD nº 2, de 27 janeiro de 2022.

A regulamentação dessa norma propiciou um ambiente mais favorável ao cumprimento da legislação de proteção de dados, trazendo

19 E-BOOK. DPO (Encarregado) Gestão dos programas de privacidade e proteção de dados – Agosto de 2021. Opice Blum. Disponível em https://opiceblum.com.br/wp-content/uploads/2019/07/EBOOK-DPO-ENCARREGADO-3.pdf Acesso em: 10 abr. 2024.

equilíbrio à possibilidade operacional e de recursos das pequenas e médias empresas com a efetivação dos direitos e das liberdades dos titulares.

Sob tal prospectiva, o Conselho Diretor da Autoridade Nacional de Proteção de Dados – ANPD admitiu que a diminuição de carga regulatória assim como o estímulo à inovação são fatores essenciais ao desenvolvimento destes negócios.[20]

5. A IMPORTÂNCIA DO ENCARREGADO DE DADOS

Relevante dizer ainda que, no que tange à dispensa de indicação de Encarregado para agentes de tratamento de pequeno porte, em que pese a relevância da atuação do Encarregado na relação de governança em privacidade, a sua falta não representa, necessariamente, um obstáculo ao atendimento dos demais requisitos trazidos pela LGPD. Tal porque, partindo do ponto de que o Encarregado de tratamento de dados (DPO) é um facilitador, mas não um viabilizador do canal de comunicação entre as partes envolvidas.

Tanto é que a carência de designação de Encarregado por agentes de tratamento (exceto aqueles descritos em Lei, os de pequeno porte) gera às empresas e organizações uma infração sancionável da Lei Geral de Proteção de Dados Pessoais de menor gravidade.

Ou seja, para a Lei de Proteção de Dados Pessoais brasileira, dada a devida importância que merece o cargo do Encarregado de tratamento de dados, a flexibilização para pequenas e médias empresas (aquelas acolhidas pela Lei) de dispensa do profissional DPO – *Data Protection Officer,* não trará prejuízo aos titulares dos dados, respeitando o critério de implementar o canal de comunicação para os clientes/titulares.

20 SEBRAE. LGPD: qual o impacto nos pequenos negócios? Sua pequena empresa está preparada. Disponível em https://www.sebrae-sc.com.br/blog/lgpd-qual-o-impacto-nos-pequenos-negocios-sua-pequena-empresa-esta-preparada Acesso em: 15 abr. 2024.

Assim, neste cenário dos "pequenos negócios", podemos afirmar que a Autoridade Nacional de Proteção de Dados – ANPD, por meio da Resolução CD/ANPD nº 2, de 27 janeiro de 2022, está dizendo que é possível atender a todos os comandos legais, em especial os direitos dos tutelados, mesmo sem a presença do Encarregado/DPO, em caso de agentes de tratamento de pequeno porte.

6. O QUE FAZ O ENCARREGADO DE DADOS

A figura do Encarregado de tratamento de dados pessoais foi criada com base no *Data Protection Officer* (DPO), previsto no Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês), que vigora na União Europeia.

O seu papel é fulcral dentro do sistema de tratamento dos dados pessoais, sendo suas funções definidas pela Lei Geral de Proteção de Dados, artigo 41, §2ª, para:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da autoridade nacional e adotar providências;
- orientar os empregados e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Além da diretriz do artigo 41, parágrafo 2º, da LGDP, foi publicada, recentemente, pela ANPD a Resolução n.º18, de 16 de julho de 2024[21], que também detalha as atribuições e atividades do Encarregado pelo tratamento de dados pessoais. É possível encontrar

21 BRASIL. Resolução CD/ANPD n.º 18, de 16 de julho de 2024. Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais, DF: Diário Oficial da União de 2024. Disponível em www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074 . Acesso em: 25 de Julho. 2024.

nesta norma a definição e as características do Encarregado, como se dará a sua indicação e a divulgação de sua contratação, disciplinando ainda sobre como evitar o conflito de interesse, dentre outros.

Mas antes de continuarmos a discorrer acerca do Encarregado de tratamento de dados pessoais, faz-se necessário trazer também, mesmo que sucintamente, como forma de darmos seguimento ao entendimento deste sujeito (Encarregado), as figuras formadoras dessa relação jurídica na conjuntura do tratamento dos dados de pessoas.

O primeiro deles é o "Titular de Dados", indivíduo de quem ou sobre quem as informações estão sendo coletadas e utilizadas. Já quem se beneficia do tratamento de determinados dados pessoais chamamos de "Controlador". Ele, o Controlador, toma todas as decisões relacionadas ao processamento dos dados pessoais, como finalidade de sua utilização, quais dados serão utilizados, onde serão armazenados e por quanto tempo serão guardados ou eliminados.

Temos ainda o "Operador" que, por sua vez, é aquela figura que essencialmente presta serviços em nome e para o Controlador, executando as atividades de processamento dos dados pessoais.

E, por fim, voltamos ao "Encarregado" – "*Data Protection Officer*" (DPO), também considerado por alguns como agente de tratamento de dados, é aquele indicado pelo Controlador, podendo ser pessoa natural ou jurídica, que consiste como canal de comunicação entre o agente de tratamento, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD). E deve atuar em conjunto com o Controlador e o Operador, porém, possui autonomia técnica no desenvolvimento de suas funções.

Este profissional precisa estar habilitado a responder na língua português, e a sua contratação, impreterivelmente, deve ser formalizada pela empresa com o registro específico de suas atribuições.

Para melhor visualizarmos o papel do Encarregado trouxemos a leitura da Marcella Costa e Ana Catarina que diz[22]:

22 E-BOOK. DPO (Encarregado) Gestão dos programas de privacidade e proteção de dados – Agosto de 2021. Artigo Privacy by Design e Privacy by Default, por Marcella Costa e Ana Catarina de Alencar. Opice Blum. Disponível em https://opiceblum.com.br/wp-content/uploads/2019/07/EBOOK-DPO-ENCARREGADO-3.pdf Acesso em: 10 abr. 2024.

> Assim, é papel do DPO direcionar ações orientadas por esse conceito na própria estrutura de governança da empresa, envolvendo todas as partes interessadas. Desse modo, a incorporação de estratégias de privacidade no negócio poderá ser atingida mais facilmente, tendo em vista que representará um componente essencial da própria estrutura de governança interna.

As autoras acima mencionadas nos fazem pensar no tamanho e na dimensão deste agente de tratamento de dados (Encarregado) na estrutura da empresa ou organização, uma vez que ele exerce a função de garantir o cumprimento da Lei Geral de Proteção de Dados Pessoais e serve como ponto de contato entre o Controlador, os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Veja que, o Encarregado, ou DPO (*Data Protection Officer*), não precisa ser necessariamente um empregado da empresa ou organização, mas carece ter total conhecimento sobre o acervo que envolve dados pessoais dentro da empresa. Isso pois o Encarregado deve organizar os fluxos de retorno às requisições de titulares, garantindo respostas adequadas e em tempo hábil, e, para tanto, deve desenvolver programas de canais de comunicação com os titulares de dados de forma a diminuir os riscos no tratamento dos dados pessoais.

As normas vigentes não determinam qual a área de atuação do Encarregado ou DPO, contudo, na prática, o referido cargo tem sido ocupado por advogados, consultores e profissionais de segurança da informação. É certo que a multidisciplinaridade é um fator primordial para a boa execução das atividades do Encarregado/DPO, dado que, dependendo da área de formação, pode este desempenhar desde a análise e elaboração de contratos, até fazer recomendações técnicas e específicas sobre infraestrutura organizacional da empresa quanto ao tratamento de dados pessoais.

O Encarregado não é responsável pelo tratamento irregular dos dados, sendo certo que as responsabilidades civil e administrativa estão, em regra, limitadas aos agentes de tratamento – Controlador

e Operador, exceto nas situações em que o Encarregado assuma a condição de Controlador de dados. A responsabilidade do Encarregado/DPO está restrita ao exercício adequado de suas funções.

Portanto, que fique cristalino o dever do Encarregado dentro da empresa ou organização para que se possa distinguir a sua funcionalidade, e, assim, optar por aderir esta figura, ou não, ao quadro participativo da empresa de pequeno e/ou médio porte que possua, é claro, os requisitos necessários à flexibilização da dispensa deste profissional.

Assim, por todos os atributos transferidos ao Encarregado acima mencionados e levando em consideração os percalços que a pequena e média empresa enfrentam no mundo dos negócios, cabe ao empresário de pequeno porte decidir pela dispensa ou aderência da figura do Encarregado em sua empresa.

Sob este olhar, é relevante reafirmar que a flexibilização da lei no que se refere à dispensa do Encarregado consiste em uma opção, uma escolha pela pequena e/ou média empresa que se enquadra nos parâmetros da lei em aderir ou não essa figura como parte de sua estrutura organizacional de tratamento de dados pessoais.

7. BOAS PRÁTICAS NA CONTRATAÇÃO DO ENCARREGADO DE DADOS

Contudo, neste cenário, no qual a norma permite ao agente de tratamento de pequeno porte a preferência de introduzir ou não o papel do Encarregado (DPO), repita-se, é de se observar cuidadosamente os direitos dos titulares, adotando 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. (Artigo 46 da LGPD).

Porquanto, não está o agente de tratamento de pequeno porte adstrito de punições caso algum direito dos titulares de dados seja lesionado por falta de cuidado daquele detentor responsável para tanto.

E, por tais premissas, é que ainda veremos empresas de médio e pequeno porte aderindo à figura do Encarregado de tratamento de dados, visto que a composição deste profissional à estrutura organizacional da empresa lhe garante que as transações de dados pessoais serão realizadas com maior seguridade possível.

Por conseguinte, vale a pena descrever acerca das boas práticas de implementação do Encarregado de tratamento de dados pessoais nas empresas de pequeno e médio porte, caso elas queiram aderir a esse personagem.

De acordo com as normas de proteção de dados, não há requisito formal exigível para a escolha do Encarregado (DPO), todavia o bom senso diz que a especialização na área de proteção de dados pessoais é um dos pressupostos mais valiosos.

Neste contexto, para a escolha do cargo de Encarregado de tratamento de dados pessoais, seja ele pessoa física ou jurídica, é de se observar o seu conhecimento acerca das leis que giram em torno da proteção de dados pessoais e o seu domínio à adequação da Lei Geral de Proteção de Dados Pessoais dentro das empresas e organizações.

E digo mais, a nosso ver, o Encarregado precisa ter a capacidade de gerir pessoas e projetos, de inovar, de ser analítico e apreciar dados, posto que é ele o responsável por estruturar iniciativas de conscientização sobre o tema proteção de dados, fornecendo treinamento adequado às equipes, e a receber da empresa as reclamações e críticas advindas dos titulares e repassá-las no prazo legal.

É importante que este profissional esteja atento à estrutura e organização da empresa, bem como sua função e seu objeto, já que é tarefa do Encarregado realizar o planejamento de como será o registro das operações de tratamento de dados pessoais; atribuir qual conteúdo, formato, público-alvo e demais detalhes do Plano de Treinamento e Comunicação em Proteção de Dados, sendo tudo isso, de acordo com os riscos verificados dentro de cada área e/ou posição específica.

8. ATRIBUIÇÕES DO ENCARREGADO DE DADOS

Como vimos acima, o Encarregado/DPO, entre as suas variadas atribuições, deve estar à frente da elaboração do Plano de Treinamento e Comunicação em Proteção de Dados, fazendo efetivamente valer o que se propõe o alusivo plano.

A implementação de um Plano de Treinamento e Comunicação em Proteção de Dados é determinante para garantir que todos os envolvidos dentro da empresa ou organização estejam cientes das responsabilidades e práticas relativas à segurança dos dados pessoais ali tratados.

Lembre-se de que o Plano de Treinamento e Comunicação é um documento, um guia para todas as atividades relacionadas ao treinamento dos empregados da empresa e à comunicação interna entre eles, com campanhas e ações educativas. Vislumbrando essa boa prática de gestão, deixo abaixo algumas dicas[23] sobre o que não pode faltar no plano de treinamento e comunicação em proteção de dados eficaz.

Vejamos:

- Explicação sobre objetivos da LGPD;
- Descrição dos seus princípios básicos e como se aplicam à realidade da empresa;
- Explicação abrangente sobre a Política de Privacidade da empresa e outros documentos aplicáveis; e
- Informações sobre canais de comunicação para dúvidas e/ou reporte de incidentes.

Ademais, é fundamental que se considere os recursos disponíveis da empresa para implementar o plano; isso inclui orçamento, equipe e ferramentas de comunicação.

23 E-BOOK. DPO (Encarregado) Gestão dos programas de privacidade e proteção de dados – Agosto de 2021. Artigo Privacy by Design e Privacy by Default, por Marcella Costa e Ana Catarina de Alencar. Opice Blum. Disponível em https://opiceblum.com.br/wp-content/uploads/2019/07/EBOOK-DPO-ENCARREGADO-3.pdf Acesso em: 10 abr. 2024.

Caso tenha dificuldade em iniciar o documento em questão, sugerimos ao Encarregado/DPO que realize em um primeiro momento uma análise e levantamento das necessidades de treinamento dentro da empresa ou organização; que conheça o perfil dos empregados da empresa ou organização para adequar a linguagem e o formato do material que será repassado a eles; e, por fim, que monitore o processo e o desenvolvimento desse projeto para que possa ser realizado ajustes, caso necessário.

O Plano de Treinamento e Comunicação parece ser trabalhoso em sua elaboração e implementação, porém é uma ferramenta utilizada pelo Encarregado, que, definitivamente, vai diferenciar a empresa no mundo dos negócios.

9. DIVULGAÇÃO DO CONTATO DO ENCARREGADO DE DADOS

Retomando ao profissional do Encarregado (DPO), inevitável dizer que, ao contratá-lo, a empresa deverá divulgar publicamente, de forma nítida e objetiva, preferencialmente no sítio eletrônico do Controlador, a identidade e as informações de contato do Encarregado. Isso porque, como já dito, o Encarregado é o meio de comunicação entre a empresa/controlador, o titular de dados e a Autoridade Nacional de Proteção de Dados - ANPD, e, portanto, a sua figura deve ser de conhecimento de todos os envolvidos, da mesma maneira o acesso a ele deve ser fácil e certo.

E, por tudo que foi dito, optando ou não pela contratação do Encarregado (DPO), a empresa precisa, necessariamente, implementar um canal específico de comunicação entre a empresa, (ver artigo número 4 – Sobre Incidentes de Segurança), o titular de dados e a agência nacional de proteção de dados. O qual deve satisfazer todos os anseios dos titulares e da sociedade em geral e ainda prestar contas à Agência Nacional de Proteção de Dados - ANPD.

10. APRENDA COM UM CASO CONCRETO: APLICAÇÃO DE PENALIDADE

Por fim, quero deixar um caso concreto como exemplo a pequenas e médias empresas para que se adaptem às normas da Lei Geral de Proteção de Dados Pessoais, no que lhes couber, o quanto antes, uma vez que a ANPD está atuante para organizações de todos os tamanhos, não se limitando apenas às maiores do mercado.

Sobre o caso concreto:[24]

Em julho de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) aplicou a primeira multa por descumprimento da norma protetiva de dados pessoais. E, pasme! A citada sanção/penalidade foi direcionada a um agente de pequeno porte, e não sobre alguma grande empresa multinacional.

Trata-se de o caso de uma microempresa do setor privado que atua como provedora de serviços de telefonia, cuja sanção foi imposta por ter essa empresa oferecido uma lista de contatos de WhatsApp de eleitores aos candidatos das eleições municipais de Ubatuba/SP, com o objetivo de propagar material de campanha eleitoral, sem a observância da norma de proteção de dados.

O processo administrativo deu início por meio de um ofício do Ministério Público de São Paulo, representado pela Promotoria de Justiça de Ubatuba, que denunciou a atividade irregular da microempresa. Com isso, a ANPD verificou que o tratamento de dados pessoais denunciado estava ocorrendo sem respaldo legal. Foi apurada ainda a falta de comprovação da indicação de Encarregado pelo tratamento de dados pessoais pela empresa. E, embora o agente de tratamento de dados pessoais fosse uma microempresa, não restou comprovado que ela (microempresa) não fazia tratamento de alto risco; condição esta necessária para excepcionalizar a exigência de designação do encarregado.

24 GOV BR. Ministério da Justiça e Segurança Nacional. Primeira multa por descumprimento a LGPD. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpdAcesso em: 14 abr. 2024.

Diante dos indícios de infração à Lei Geral de Proteção de Dados Pessoais e do não atendimento de determinações da equipe de fiscalização pela empresa, a Autoridade Nacional de Proteção de Dados – ANPD lavrou Auto de Infração, iniciando o Processo Administrativo Sancionador. Em seguida a microempresa foi notificada da lavratura de Auto de Infração e apresentou sua defesa.

Finalizada a instrução, a CGF/ANPD concluiu pela ocorrência de infração ao artigo 7º e ao artigo 41 da LGPD, e artigo 5º da Resolução CD/ANPD nº 1/2021, aplicando a multa no valor para cada infração limitada a 2% (dois por cento) do seu faturamento bruto, conforme art. 52, II, da LGPD, totalizando a soma de R$14.400,00 (quatorze mil e quatrocentos reais).

Esta situação cabe como uma recomendação, um alerta para os agentes de pequeno porte acerca da importância de estarem em conformidade com a Lei Geral de Proteção de Dados Pessoais, implementando política de boas práticas e governança dentro da empresa. Sendo certo que a figura do Encarregado, mesmo que não obrigatória em alguns casos, é considerada uma medida responsável e alinhada aos princípios de proteção de dados.

Ou seja, apesar das flexibilizações introduzidas pela Resolução CD/ANPD 2, de 27 janeiro de 2022, a relevância da comunicação com os titulares dos dados e o acolhimento de práticas responsáveis de governança ainda continuam sendo fundamentais para garantir a proteção eficaz dos dados pessoais e o cumprimento dos direitos dos indivíduos.

11. CONCLUSÃO

A Lei Geral de Proteção de Dados Pessoais – LGPD tenta oferecer maior segurança às informações pessoais dos indivíduos, obrigando os agentes de tratamento de dados (empresas e organizações) a criarem mecanismos de proteção para amenizar os riscos de vazamento dos dados pessoais ou utilização indevida desses dados.

Ocorre que a rigidez da LGPD trouxe peso aos agentes de pequeno porte, tanto no que diz respeito ao cumprimento desta

norma quanto no que se refere às sanções aplicadas por ela àqueles que a descumprirem. Isso em razão do tamanho e eventuais limitações das pequenas e médias empresas, que, muitas vezes, não possuem condições de contratar profissionais especializados em tratamento de dados pessoais e segurança da informação.

Ora, as empresas e organizações, além das sanções administrativas previstas na LGPD, como multa, bloqueios, suspensão do funcionamento do banco de dados e até mesmo proibição do exercício da atividade relacionada ao tratamento de dados, podem ainda sofrer em responder por demandas judiciais dos titulares dos dados, que têm o direito de buscar indenizações por danos materiais e/ou morais causados em virtude do descumprimento da lei.

Dessa feita, visando atender aos agentes de tratamento de pequeno porte, em face da rigidez da LGPD, de maneira mais acessível e apropriada às suas realidades, sem, contudo, ferir o direito dos titulares de dados pessoais na utilização de seus dados, surge a Resolução CD/ANPD nº 2, de 27 janeiro de 2022. Esta norma, entre outros, definiu quem são os agentes de pequeno porte e quais desses agentes poderão se beneficiar da flexibilização da norma brasileira de proteção de dados.

Neste artigo enfatizamos a flexibilização da norma de proteção de dados concernente à dispensa da obrigação de algumas pequenas e médias empresas em nomear um DPO/Encarregado de tratamento de dados pessoais. Profissional este de tamanha importância ante o conjunto de ações que impactam todo o ambiente institucional das empresas, com o propósito de prevenir os riscos, detectar e combater as ameaças digitais.

As micro e pequenas empresas – exceto aquelas que continuam sendo obrigadas pela lei – podem até optar por não ter a figura do encarregado em sua empresa, porém estão compelidas a criar e manter um canal de comunicação entre a empresa, o titular de dados e a agência nacional de proteção de dados. Veja que a lei reduziu para aqueles, os agentes de pequeno porte, a figura do Encarregado de dados pessoais quando permitiu que apenas o canal de comunicação

fosse suficiente para atender às demandas advindas da segurança de informação e dados pessoais.

Todavia, por tudo que vimos, a comunicação sobre a disposição/manuseio de dados pessoais nas empresas não se resume apenas a marketing e publicidade, mas compreende em outras maneiras de interação e relacionamento com os titulares de dados pessoais e com os próprios empregados da empresa.

E, apesar de muitas empresas de pequeno e médio porte ainda não terem maturidade para a adequação da LGPD, seja por sua estrutura organizacional ou financeira, o papel do Encarregado continua a ser essencial. Trata-se da melhor prática para o gerenciamento de riscos no âmbito da segurança da informação/dados pessoais, uma vez que eles enxergam para além de receber denúncias dos usuários e podem repassar informações padronizadas.

Isso porque o Encarregado/DPO é dinâmico, multidisciplinar e age de forma preventiva, aplicando as melhores práticas dentro da empresa ou organização no atendimento às requisições das pessoas, observando as particularidades dos empregados e dos titulares de dados.

Neste sentido, para as micro e pequenas empresas fica o dilema quanto à possibilidade de adotar somente o canal de comunicação exigido por lei, ou investir um pouco mais no profissional qualificado para exercer a função de Encarregado de dados pessoais e, dessa forma, garantir maior seguridade à empresa no que tange ao manuseio de dados pessoais, evitando as severas sanções da Autoridade Nacional de Proteção de Dados e/ou possíveis demandas judiciais.

Ademais, no atual cenário digital, sensível à privacidade de dados, cujo mercado está repleto de oportunistas a ganhar vantagem, em especial, financeira, as empresas sejam elas de grande porte ou pequenos negócios, têm gigantesco papel a garantir o máximo de segurança possível aos seus usuários.

Implementar um Programa de Privacidade com a aderência de um Encarregado/DPO não é somente uma obrigação legal, mas consiste em uma oportunidade de demonstrar transparência e

responsabilidade; é uma maneira de obter crédito diante dos titulares de dados e reforçar parcerias de negócios.

E implementar procedimentos eficazes de cumprir a legislação e mitigar os riscos é o primeiro passo para que possamos alterar a nossa realidade atual.

Lado outro, no mundo dos negócios, a empresa que melhor zelar por boas práticas de privacidade fortalece a confiança de seus consumidores e sai disparado à frente de seus concorrentes.

Para algumas empresas de pequeno e médio porte, a contratação de um Encarregado/DPO para o tratamento dos dados pessoais acarreta o ônus do prejuízo na sua conjuntura econômica, porém a visão de que se precisa ter é que a conformidade com a norma não necessita ser um óbice, mas, sim, uma oportunidade para revigorar a empresa e atender às expectativas de clientes, parceiros de negócios e investidores em relação à privacidade e segurança dos dados.

Portanto, de tudo que vimos por aqui acerca da possibilidade de alguns agentes de pequeno porte (micro e pequenas empresas assim definidas e especificadas pela Resolução CD/ANPD nº 2, de 27 janeiro de 2022), a optar pela dispensa do Encarregado, *Data Protection Officer* – DPO; o que fica é que contar com a presença desse profissional dentro da empresa é sempre uma boa prática para o tratamento de dados pessoais.

REFERÊNCIAS

BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 abril. 2024.

E-BOOK. DPO (Encarregado) Gestão dos programas de privacidade e proteção de dados – Agosto de 2021. Artigo Privacy by Design e Privacy by Default, por Marcella Costa e Ana Catarina de Alencar. Opice Blum. Disponível em https://opiceblum.com.br/wp-content/uploads/2019/07/EBOOK-DPO-ENCARREGADO-3.pdf Acesso em: 10 abr. 2024.

E-BOOK. O Encarregado Pelo Tratamento de Dados Pessoais (DPO) Em Infográfico, março 2022. Opice Blum. Disponível em https://opiceblum.com.br/wp-content/uploads/2022/02/cartilha_DPO_marco_versao_final.pdf Acesso em: 10 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº 2, de 27 de janeiro de 2002. Imprensa Nacional. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper . Acesso em: 14 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Primeira multa por descumprimento a LGPD. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpdAcesso em: 14 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº1, de 28 de outubro de 2021. Imprensa Nacional. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021 Acesso em: 14 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Segurança Da Informação Para Agentes De Tratamento De Pequeno Porte, Versão 1.0, out. 2021, Capa atualizada para atendimento à Legislação Eleitoral 2022; Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdfAcesso em: 15 abr.2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD n.º 18, de 16 de julho de 2024. Imprensa Nacional. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074 Acesso em: 25 jul. 2024.

SEBRAE. LGPD: qual o impacto nos pequenos negócios? Sua pequena empresa está preparada. Disponível em https://www.sebrae-sc.com.br/blog/lgpd-qual-o-impacto-nos-pequenos-negocios-sua-pequena-empresa-esta-preparada Acesso em: 15 abr. 2024.

CAPÍTULO 4

LGPD E OS INCIDENTES DE SEGURANÇA: COMO AS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE PODEM SE PROTEGER E COMO AGIR EM CASO DE CONFIRMAÇÃO DE INCIDENTE

Jéssica Lorena da Silva Pinheiro[25]

RESUMO: O presente estudo, baseado na Lei Geral de Proteção de Dados Pessoais - LGPD[26], Regulamentos e guias orientativos elaborados pela Autoridade Nacional de Proteção de dados - ANPD, traz uma análise simples e dinâmica sobre como as Microempresas e Empresas de Pequeno Porte podem se proteger e se adaptar perante a LGPD para mitigar riscos de ocorrência de incidentes de segurança. Sabemos que, mesmo se adotado as mais diversas medidas de proteção, em se tratando de incidentes de segurança, especialmente os cibernéticos, diariamente, surgem novos desafios que colocam as organizações em situação de vulnerabilidade e precisam ser enfrentados. Nesse sentido, trazemos orientações aos agentes de pequeno porte, acerca da comunicação à ANPD e aos Titulares dos Dados, nos casos de confirmação de um incidente de segurança, para cumprimento dos requisitos legais.

PALAVRAS-CHAVE: LGPD - Incidente de Segurança - Incidente Cibernético - Medidas de Proteção - Mitigação de Riscos - Flexibilizações para agentes de pequeno porte - Formulário CIS.

ABSTRACT: This study, based on the General Personal Data Protection Law - LGPD, Regulations and guidance guides prepared by the National Data Protection Authority - ANPD, brings a simple and dynamic analysis on how Micro and Small Businesses can protect themselves and adapt to the LGPD, to mitigate risks of security incidents occurring. We know that, even if adopting the most diverse protection measures, when it comes to security incidents, especially cyber incidents, new challenges arise daily that place organizations

25 Jéssica Lorena da Silva Pinheiro: Advogada e bacharel em Direito pela Universidade de Itaúna/MG, Analista Jurídica Sênior Generalista e em Privacidade/Proteção de Dados. Pós-graduanda em Direito Digital e Proteção de Dados pela Ebradi. Membro da Comissão de Proteção de Dados da OAB/MG Subseção Betim. @advjessicapinheiro

26 BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 25 abr. 2024.

in a vulnerable situation and need to be faced. In this sense, we bring guidance to small agents, regarding communication to the ANPD and Data Holders, in cases of confirmation of a security incident, to comply with legal requirements.

KEYWORDS: LGPD - Security Incident - Cyber Incident - Protection Measures - Risk Mitigation - Flexibility for small agents - CIS Form.

1. INTRODUÇÃO

Com o mundo globalizado e informatizado, dados e informações pessoais estão circulando cada vez mais, sem qualquer controle, contribuindo para que as pessoas fiquem expostas aos mais diversos públicos e riscos.

Quem nunca se deparou com uma ligação ou recebeu um e-mail indesejado, com ofertas de empréstimos, promoções ou até mesmo com tentativas de golpes? Como foi possível o acesso a estas informações e/ou dados pessoais?

Visando à regulamentação e proteção dos direitos e garantias fundamentais da pessoa humana, a Lei Geral de Proteção de Dados Pessoais, nº 13.709 de 2018, estabeleceu mecanismos para o tratamento de dados pessoais, por pessoas naturais ou jurídicas, nos moldes do art. 3º da referida lei.

Apesar de a LGPD ter entrado em vigor em 2020, sua aplicabilidade foi acontecendo de forma gradual, tendo em vista a complexidade e a necessidade de adequação à realidade do nosso País.

Até aqui, qualquer pessoa, natural ou jurídica, que realizasse tratamento de dados pessoais, para fins econômicos, deveria se adaptar ao que determina a LGPD, sem qualquer exceção.

Ocorre que a adequação nos exatos moldes previstos na Lei 13.709/2018 mostrou-se inviável àqueles que exerciam o tratamento de dados pessoais para fins econômicos, mas que não possuíam estrutura

física, nem financeira, como as empresas de médio e grande porte ou multinacionais, por exemplo.

Então, a partir de consultas públicas, realizadas para debates e manifestações da sociedade quanto à regulamentação da lei, o Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD), em 27 de janeiro de 2022, por meio da Resolução CD/ANPD nº 2, aprovou o regulamento de aplicação da Lei 13.709, de 14 de agosto de 2018, para agentes de tratamento de pequeno porte[27].

A referida resolução trouxe flexibilizações aos requisitos da LGPD, para viabilizar a adequação das microempresas e empresas de pequeno porte[28].

Outra novidade foi a recente publicação da Resolução CD/ANPD nº 15, em 24 de abril de 2024[29], estabelecendo importantes diretrizes para o procedimento de Comunicação de Incidente de Segurança à ANPD e aos titulares dos dados pessoais.

Nesse sentido, buscando facilitação ao entendimento da Lei Geral de Proteção de Dados, neste capítulo iremos abordar, de forma dinâmica, os meios e mecanismos a serem adotados, em casos

27 GOV BR. Ministério da Justiça e Segurança Nacional . Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte, DF: Diário Oficial da União de 2022. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 19 abr. 2024.

28 GOV BR. Ministério da Justiça e Segurança Nacional. O artigo 2º, inciso II da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022 estabeleceu que microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, sociedade limitada unipessoal, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e 18-A, §1º da Lei Complementar nº 123, de 14 de dezembro de 2006. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 19 abr. 2024.

29 GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº 15, de 24 de abril de 20224. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 11 mai. 2024.

de incidentes de segurança envolvendo agentes de tratamento de pequeno porte.

2. OS INCIDENTES DE SEGURANÇA E A LGPD:

Em que pese a LGPD, em seu artigo 48, tratar sobre incidentes de segurança, pairavam diversas dúvidas quanto aos prazos, procedimentos e definições que deveriam ser adotados pelos agentes de tratamento, em casos suspeitos ou confirmados de incidentes de segurança, em virtude da ausência de regulamentação específica sobre o tema.

Nesse sentido, em 24 de abril de 2024, um novo marco histórico foi estabelecido para a Lei Geral de Proteção de Dados Pessoais no Brasil, por meio da Resolução CD/ANPD nº 15, que aprovou o Regulamento de Comunicação de Incidente de Segurança.

A partir deste regulamento, é possível, com maior clareza e segurança, seguir os procedimentos estabelecidos pela ANPD, para Comunicação de Incidentes envolvendo dados pessoais, que possam acarretar riscos ou danos relevantes aos titulares[30].

Segundo o art. 3º, Inciso XII, da Resolução nº 15, o incidente de segurança se define como qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

Já nas palavras de Artur SABBAT, diretor do Conselho Diretor da ANPD, "o incidente de segurança caracteriza-se pela confirmação de violação à segurança de dados pessoais, como acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados inadequada ou

30 GOV BR. Ministério da Justiça e Segurança Nacional. Art. 1º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança, DF: Diário Oficial da União de 2024. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 11 mai. 2024.

ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados"[31].

Ou seja, sempre que o agente de tratamento de dados tomar conhecimento da ocorrência de acesso, divulgação, perda ou alteração indevida de dados pessoais aos quais é responsável pela integridade e proteção da informação, deverá, imediatamente, avaliar os possíveis danos e iniciar, se for o caso, as medidas de reparações.

Para o efetivo cumprimento do que determina a legislação para a proteção de dados pessoais pelos agentes de tratamento, necessário se faz a adequação e implantação de procedimentos que possibilitem a segurança dos dados e informações utilizadas, seja de seus empregados, clientes ou de terceiros que estejam vinculados às suas atividades empresariais.

Visando possibilitar às microempresas e empresas de pequeno porte esse efetivo cumprimento das normas previstas na LGPD, a ANPD tratou sobre a flexibilização ou procedimento simplificado de incidente de segurança para estes agentes de tratamento[32].

Assim, além das flexibilizações, por exemplo, quanto à dispensa de indicação de Encarregado pelo Tratamento de Dados e autorização para estabelecer políticas simplificadas de segurança da informação, a Resolução nº 2 da ANPD, em seu artigo 14, inciso II, concedeu prazos em dobro ao agente de tratamento de pequeno porte, para comunicação ao órgão fiscalizador e ao titular sobre a ocorrência do incidente de segurança.

Baseado nestas considerações, analisaremos adiante, alternativas simples e eficazes, para mitigação dos riscos ou reversão dos efeitos gerados em incidentes de segurança.

---

31 GOV BR. Ministério da Justiça e Segurança Nacional. Incidentes de Segurança com Dados Pessoais. SABBAT, Artur. Definição disponível em https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Acesso em: 19 abr. 2024.

32 Art. 10 da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte, DF: Diário Oficial da União de 2022. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 20 abr. 2024.

3. COMO AS EMPRESAS DE PEQUENO PORTE E MICROEMPRESAS PODEM SE PROTEGER DOS INCIDENTES DE SEGURANÇA?

São grandes os desafios para que as empresas se protejam dos riscos aos quais estão expostas, quando o assunto é a segurança de dados pessoais.

Com a efetiva regulamentação da Proteção de Dados em nosso País, o cumprimento das normas previstas na LGPD passou a ser tão importante quanto o cumprimento das obrigações trabalhistas, fiscais e tributárias, por exemplo.

Para a efetividade da norma, faz-se necessário que o tema se torne parte da cultura e política organizacionais e seja vivenciado pela empresa e seus empregados, como algo corriqueiro ao cotidiano.

Em um breve resumo, quanto à proteção de dados pessoais e, consequentemente, redução dos riscos de ocorrência de incidentes de segurança, destaca-se o artigo 46 da LGPD, que estabelece que compete ao controlador e ao operador adotar medidas de segurança, 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.

Abaixo, destacamos algumas formas comuns de ocorrência de incidentes de segurança, descritos no Formulário de Comunicação de Incidente de Segurança com dados pessoais[33:]

- Sequestro de Dados (ransomware) sem transferência de informações;
- Sequestro de Dados (*ransomware*) com transferência e/ou publicação de informações;

33 FORMULÁRIO CIS (Formulário de Comunicação de Incidente de Segurança com dados pessoais). Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx. Acesso em: 20 abr. 2024

- Exploração de vulnerabilidade em sistemas de informação;
- Vírus de Computador / *Malware*;
- Roubo de credenciais / Engenharia Social;
- Violação de credencial por força bruta;
- Publicação não intencional de dados pessoais;
- Divulgação indevida de dados pessoais;
- Envio de dados a destinatário incorreto;
- Negação de Serviço (DoS);
- Acesso não autorizado a sistemas de informação;
- Alteração/exclusão não autorizada de dados;
- Perda/roubo de documentos ou dispositivos eletrônicos;
- Descarte incorreto de documentos ou dispositivos eletrônicos;
- Falha em equipamento (hardware);
- Falha em sistema de informação (*software*);
- Outro tipo de incidente cibernético;
- Outro tipo de incidente não cibernético;

Vale ressaltar ainda que os incidentes de segurança podem acontecer das mais variadas formas, e não somente por meios digitais.

Em importante exercício de Simulação de Resposta a Incidente Cibernéticos, realizado pela FIESP em parceria com o Senai e apoio da Agência Nacional de Proteção de Dados e do Gabinete de Segurança Institucional da Presidência da República (GSI), a ANPD destacou que nem todo incidente de segurança envolve falhas em sistemas de informação. Eles também podem ocorrer por meio de[34]:

34 FIESP. Exercício de Simulação de Resposta a Incidente Cibernético. Disponível em https://www.youtube.com/watch?v=KJWU1f6RAxg. Acesso em: 18 abr. 2024

- Envio incorreto de e-mails;
- Publicação não intencional de dados;
- Revelação de informação indevida por meio de ligação telefônica;
- Roubo/Perda de equipamento/documento físico;
- Aliciamento de empregados com credenciais válidas;
- Reaproveitamento de credenciais roubadas;

Assim, os agentes de tratamento devem buscar mecanismos de segurança para proteger os dados dos titulares, vinculados aos seus negócios ou atividades.

Importante frisar que sofrer um incidente de segurança não significa, necessariamente, infringir a LGPD ou outras normas[35].

Mesmo adotando as mais diversas medidas de proteção, em se tratando de incidentes cibernéticos, por exemplo, a verdade é que os ataques são cada vez mais complexos, e os criminosos estão cada vez mais profissionais, colocando todas as organizações em situação de vulnerabilidade, tornando-as também vítimas destas situações[36].

Apesar de tais complexidades para a adoção de medidas de segurança, suficientes ao atendimento dos requisitos da LGPD, há soluções simples e eficazes que podem e devem ser utilizadas pelas Microempresas ou Empresas de Pequeno Porte, para a proteção de dados pessoais, com baixos custos e que auxiliarão na mitigação dos riscos de ocorrências de incidentes de segurança.

Elencamos abaixo, algumas ações[37]:

35 FIESP. Exercício de Simulação de Resposta a Incidente Cibernético. Disponível em https://www.youtube.com/watch?v=KJWU1f6RAxg. Acesso em: 18 abr. 2024

36 FIESP. Exercício de Simulação de Resposta a Incidente Cibernético. Disponível em https://www.youtube.com/watch?v=KJWU1f6RAxg. Acesso em: 18 abr. 2024

37 GOV BR. Ministério da Justiça e Segurança Nacional. ANPD. Guia orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf .Acesso em: 20 abr. 2024.

- Criação de Políticas de Segurança da Informação, ainda que de forma simplificada, que estabeleça diretrizes aos usuários para o tratamento de dados pessoais;
- Definições quanto à utilização de senhas alfanuméricas com caracteres especiais, armazenando-as, se necessário, em locais seguros, até a sua memorização;
- Orientação sobre o não compartilhamento de logins e senhas de acesso das estações de trabalho;
- Utilização de antivírus e atualização recorrente de softwares para evitar vulnerabilidades passíveis de invasões e acessos maliciosos;
- Estabelecimento de locais seguros para a guarda e arquivo de documentos que contenham tratamento de dados pessoais;
- Criação de controles de acesso físico;
- Realização de treinamentos e campanhas de conscientização constantes sobre segurança e proteção de dados;
- Orientação frequente aos empregados quanto à utilização de e-mails e os riscos de acesso a links e anexos desconhecidos;
- Ampla divulgação sobre a importância de comunicação imediata com os responsáveis legais da empresa, havendo possibilidade de qualquer incidente;
- Criação de múltiplos fatores de autenticação;
- Criação de cópias de segurança. (backups);
- Utilize um "firewall" e mantenha-o ativo[38];
- Não habilite macros no Microsoft Office[39].

38 PCSP. Guia de prevenção "Ransomware" (sequestro de dados). Disponível em https://www.policiacivil.sp.gov.br/portal/imagens/GUIA%20RANSONWARE%20v2.pdf. Acesso em: 21 abr. 2024.

39 PCSP. Guia de prevenção "Ransomware" (sequestro de dados). Disponível em https://www.policiacivil.sp.gov.br/portal/imagens/GUIA%20RANSONWARE%20v2.

Outra ação importante a ser observada por agentes de pequeno porte, indicada por especialistas e autoridades, é jamais realizar pagamentos para resgate, em caso de incidentes de segurança envolvendo sequestro de dados, por exemplo.

Eles explicam que não há garantia de que a vítima receberá seus dados de volta e que, pagar o valor do resgate, também pode colocá-la em risco de novos ataques, pois o invasor poderá vislumbrar a possibilidade de receber novos pagamentos[40].

É importante, nesses casos, que o responsável legal da Microempresa ou Empresa de Pequeno Porte que procure auxílio por meio de autoridades policiais e/ou profissionais qualificados, em busca de alternativas que minimizem as consequências e prejuízos do ataque.

Vale ressaltar, por fim, que os custos de investimentos em segurança da informação sempre serão infinitamente menores que os custos atrelados a um incidente de segurança podem oferecer!

Por todo o exposto, verifica-se que é possível a mitigação dos riscos de incidentes de segurança, muitas vezes, contando apenas com a própria estrutura já existente na Organização, sem a necessidade de investimentos vultuosos para adoção de medidas de proteção contra-ataques cibernéticos ou vazamento de dados.

4. DAS COMUNICAÇÕES SOBRE A OCORRÊNCIA DE UM INCIDENTE DE SEGURANÇA

A Lei Geral de Proteção de Dados Pessoais estabeleceu em seu artigo 48 que, ao ocorrer um incidente de segurança, é necessário que

pdf. Acesso em: 21 abr. 2024.

40 PCSP. Guia de prevenção "Ransomware" (sequestro de dados), pág. 04. Disponível em https://www.policiacivil.sp.gov.br/portal/imagens/GUIA%20RANSONWARE%20v2.pdf. Acesso em: 21 abr. 2024.

o Controlador comunique, dentro do prazo legal, à Agência Nacional de Proteção de Dados e ao titular do dado pessoal o fato[41].

Em que pese a obrigação da comunicação sobre a ocorrência de incidentes de segurança à ANPD e aos titulares seja do agente Controlador, é dever também do Operador comunicar ao Controlador seu conhecimento sobre quaisquer incidentes com dados pessoais que envolvam suas atividades.

Além disso, é responsabilidade de ambos (Controlador e Operador) a adoção de medidas para prevenir a ocorrência de danos aos titulares[42].

Nesse sentido, o(s) agente(s) de tratamento de dados pessoais de pequeno porte deverá(ão), imediatamente, adotar(em) medidas para apuração de possíveis dados afetados, dos riscos e extensão dos danos causados aos titulares[43].

Para apuração da ocorrência um incidente de segurança, o Controlador deverá, por meio do registro do incidente de segurança, verificar as seguintes situações[44]:

- a data de conhecimento do incidente;
- a descrição geral das circunstâncias em que o incidente ocorreu;
- a natureza e a categoria de dados afetados;

41 BRASIL. Art. 48, caput, da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 21 abr. 2024.

42 GOV BR. Ministério da Justiça e Segurança Nacional. ANPD. Comunicação de Incidente de Segurança Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 20 abr. 2024.

43 BRASIL. Art. 48, caput, da Lei 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 21 abr. 2024.

44 GOV BR. Ministério da Justiça e Segurança Nacional. Art. 10º, § 1º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 11 mai. 2024

- o número de titulares afetados;
- a avaliação do risco e os possíveis danos aos titulares;
- as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
- a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
- os motivos da ausência de comunicação, quando for o caso.

Confirmando-se que dados pessoais e/ou sensíveis foram afetados, o responsável legal do agente Controlador deverá comunicar à ANPD e aos titulares a ocorrência do incidente, adotando os critérios estabelecidos no artigo 48 da LGPD.

> 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.
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> § 2º 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.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

A Resolução CD/ANPD nº 15, regulamentou que o controlador deverá comunicar a ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares e que estes riscos ou danos devem afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios[45]:

- Dados pessoais sensíveis;
- Dados de crianças, de adolescentes ou de idosos;
- Dados financeiros;
- Dados de autenticação em sistemas;
- Dados protegidos por sigilo legal, judicial ou profissional; ou
- Dados em larga escala.

Ocorrendo quaisquer situações mencionadas acima, deverá o Controlador comunicar à ANPD, no prazo de três dias úteis a contar da data de conhecimento de que o incidente afetou dados pessoais,

45 GOV BR. Ministério da Justiça e Segurança Nacional. Art. 4º e 5º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 11 mai. 2024

ressalvados os prazos de comunicação previsto em legislação específica[46].

Tendo em vista as flexibilizações concedidas aos agentes de pequeno porte, a redação do artigo 14, inciso II, da Resolução CD/ANPD nº 2, ratificada pelo art. 6º, § 8º da Resolução CD/ANPD nº15, é garantido prazo em dobro, as microempresas e empresas de pequeno porte, que terão até 06 (seis) dias úteis, para realizar o comunicado do incidente de segurança à Agência Nacional[47].

Esta comunicação deverá ocorrer, mediante preenchimento do Formulário de Comunicação de Incidente de Segurança (CIS) [48] pelo Encarregado de tratamento de dados ou pelo responsável legal da empresa de pequeno porte, adotando os critérios contidos no art. 6º, § 2º da Resolução CD/ANPD nº 15:

- Art. 6º (...)
- § 2º A comunicação de incidente de segurança deverá conter as seguintes informações:
- I - a descrição da natureza e da categoria de dados pessoais afetados;
- II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

46 GOV BR. Ministério da Justiça e Segurança Nacional. Art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 11 mai. 2024.

47 GOV BR. Ministério da Justiça e Segurança Nacional. Art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 11 mai. 2024.

48 GOV BR. Ministério da Justiça e Segurança Nacional. Art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 11 mai. 2024.

- III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
- VII - a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;
- VIII - os dados do encarregado ou de quem represente o controlador;
- IX - a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;
- X - a identificação do operador, quando aplicável;
- XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

No formulário de comunicação de incidente de segurança também deverá ser destacado se o preenchimento das informações se dará de forma Completa, Preliminar ou Complementar:

- **Completa:** Todas as informações a respeito do incidente estão disponíveis e a comunicação aos titulares já foi realizada.
- **Preliminar:** Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a comunicação aos titulares ainda não foi realizada.

- **Complementar:** Complementação de informações prestadas em comunicação preliminar. A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.

Vale ressaltar que a comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo Controlador[49].

A complementação posterior das informações, nos termos do art. 6º, § 3º da Resolução CD/ANPD nº 15, deverá ocorrer, de maneira fundamentada, em até quarenta dias úteis, conforme flexibilização aos agentes de pequeno porte.

Faz-se necessária a preservação de todas as evidências e registros das ações adotadas para a apuração e resolução do incidente, de forma que possibilite sua posterior rastreabilidade, sempre que necessário.

Realizadas todas as apurações e o devido preenchimento do CIS, deverá o representante legal da empresa realizar o protocolo eletrônico do formulário, juntamente com todos os documentos comprobatórios relacionados à empresa e ao incidente de segurança, por meio do Sistema Único de Processo Eletrônico em Rede[50], mediante criação de login e senha, conforme instruções contidas no próprio site.

Após a finalização, um Recibo Eletrônico de Protocolo será gerado automaticamente pelo sistema e incluído no processo[51].

---

49 FORMULÁRIO CIS (Formulário de Comunicação de Incidente de Segurança com dados pessoais). Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx. Acesso em 21 abr. 2024.

50 O formulário CIS e demais documentos deverão ser protocolados no Sistema Único de Processo Eletrônico em Rede (SUPERGOV.BR). Disponível em: https://super.presidencia.gov.br/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_gerar_senha&id_orgao_acesso_externo=0. Acesso em 21 abr. 2024.

51 GOV BR. Ministério da Justiça e Segurança Nacional. ANPD. Comunicação de Incidente de Segurança Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 21 abr. 2024.

No que diz respeito aos Titulares dos Dados, a comunicação também deverá ocorrer pelo Controlador, no prazo de 06 (seis) dias úteis[52], contados do conhecimento pelo controlador de que o incidente afetou dados pessoais, e deverá conter as seguintes informações:

- a descrição da natureza e da categoria de dados pessoais afetados;
- as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
- a data do conhecimento do incidente de segurança; e
- o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

A Resolução CD/ANPD nº 15 disciplinou ainda que, na comunicação do incidente aos titulares, o Controlador deverá fazer o uso de linguagem simples e de fácil entendimento e ocorrer de forma direta e individualizada, caso seja possível identificar o titular, por meio de telefone, e-mail, mensagem eletrônica ou carta[53].

52 GOV BR. Ministério da Justiça e Segurança Nacional . Art. 9º, § 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 11 mai. 2024.

53 GOV BR. Ministério da Justiça e Segurança Nacional . Art. 9º, § 1º e 2º da Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 11 mai. 2024.

Havendo dificuldade na identificação do titular, o Controlador deverá comunicar, de forma direta e de fácil visualização, em até 06 (seis) dias úteis, pelo período de, no mínimo, três meses, por intermédio de seus meios de comunicação disponíveis (sítio eletrônico, aplicativos, mídias sociais ou canais de atendimento ao titular), a ocorrência do incidente.

Deverá ainda o Controlador, em até três dias úteis, a contar do término do prazo de envio de Comunicação à ANPD (seis dias úteis), apresentar, ao processo de comunicação de incidente de segurança, declaração de que foi realizada a comunicação aos titulares e quais os meios de contato foram utilizados.

Por fim, cumpre esclarecer que o artigo 10 da Resolução CD/ANPD nº 15, estabelece que o Controlador deverá manter o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

Durante a análise das informações do incidente apresentadas, a ANPD avaliará se a empresa adotava condições mínimas de segurança da informação e quais medidas foram adotadas para a reversão ou mitigação do impacto ao(s) titular(es) dos dados.

Nesse sentido, a principal recomendação é que o agente de pequeno porte jamais omita qualquer informação à ANPD e aos titulares dos dados, demonstrando, por meio de documentos e ações, que, caso ocorra qualquer incidente de segurança, envolvendo dados pessoais ou não, foi devido a uma fatalidade, uma vez que cumpria todas as medidas de segurança possíveis ao seu negócio.

5. CONCLUSÃO

Durante muitos anos, a disseminação desregulada de informações pessoais, a prática ilícita de venda de bancos de dados ou até mesmo o armazenamento de informações sem as devidas medidas

de segurança permitiram que pessoas e empresas tratassem diversos dados pessoais de maneira indevida e sem qualquer regulamentação.

Mesmo sem qualquer conhecimento ou consentimento dos titulares dos dados para o tratamento das informações, elas eram utilizadas livremente para fins econômicos e até mesmo ilícitos.

Além disso, os meios digitais se fazem cada vez mais presentes em nosso cotidiano e, juntamente com esta tecnologia, há mais exposições de informações e dados pessoais de forma indevida.

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais foi um marco importante para o Brasil, na regulamentação de acesso aos dados pessoais dos cidadãos brasileiros.

Com o advento da LGPD, todas as pessoas naturais e jurídicas que realizem tratamento de dados em suas atividades que tenham por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional, tem o dever de estabelecer medidas de segurança para a proteção dos dados pessoais dos titulares.

Assim, para que os agentes de pequeno porte pudessem se adaptar à LGPD, a Resolução nº 2 da ANPD flexibilizou a adoção de políticas e medidas de segurança simplificadas, levando em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte.

Tais políticas e medidas se fazem necessárias para a prevenção de ocorrência de Incidentes de Segurança.

Nesse sentido, o presente artigo apresentou soluções simples e eficazes a serem utilizadas pelos agentes de pequeno porte para a proteção de dados, com baixos custos e que auxiliarão na mitigação dos riscos de ocorrências de incidentes de segurança, utilizando-se, na maioria das vezes, recursos já existentes na Organização, sem a necessidade de investimentos vultuosos para adoção de medidas de proteção contra-ataques cibernéticos ou vazamento de dados.

Também foi destacada a importância de treinamentos e orientações aos agentes de tratamento e seus empregados sobre a proteção de arquivos e informações por meio de senhas de segurança,

sobre se ter a devida atenção ao acessar anexos e links de e-mails recebidos, importância da criação de backups, entre outros.

Salientou-se sobre os tipos de incidentes de segurança e sobre as determinações da LGPD para comunicação à ANPD e aos titulares dos dados, após a análise detalhada e confirmação do vazamento da informação.

Foram demonstrados os meios de comunicação de Incidentes aos Titulares dos Dados e apresentadas orientações sobre o preenchimento do formulário CIS, para comunicação à ANPD.

Cumpre esclarecer que a Lei Geral de Proteção de Dados Pessoais busca a proteção dos direitos e garantias fundamentais da pessoa humana. Nesse sentido, o presente artigo buscou facilitar ao agente de pequeno porte, melhor entendimento quanto aos procedimentos e requisitos a serem adotados em ocorrências de incidentes de segurança e, principalmente, como se adaptarem aos termos da LGPD.

REFERÊNCIAS

BRASIL. Lei 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais, DF: Diário Oficial da União de 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 21 abr. 2024.

FIESP. Exercício de Simulação de Resposta a Incidente Cibernético. Disponível em https://www.youtube.com/watch?v=KJWU1f6RAxg. Acesso em: 18 abr. 2024

FORMULÁRIO CIS (Formulário de Comunicação de Incidente de Segurança com dados pessoais). Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx. Acesso em: 20 abr. 2024

GOV BR. Ministério da Justiça e Segurança Nacional. ANPD. Guia orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf .Acesso em: 20 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº 2, de 27 de janeiro de 2002. Imprensa Nacional. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 19 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024 . Acesso em: 11 mai. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. Incidentes de Segurança com Dados Pessoais. SABBAT, Artur. Definição

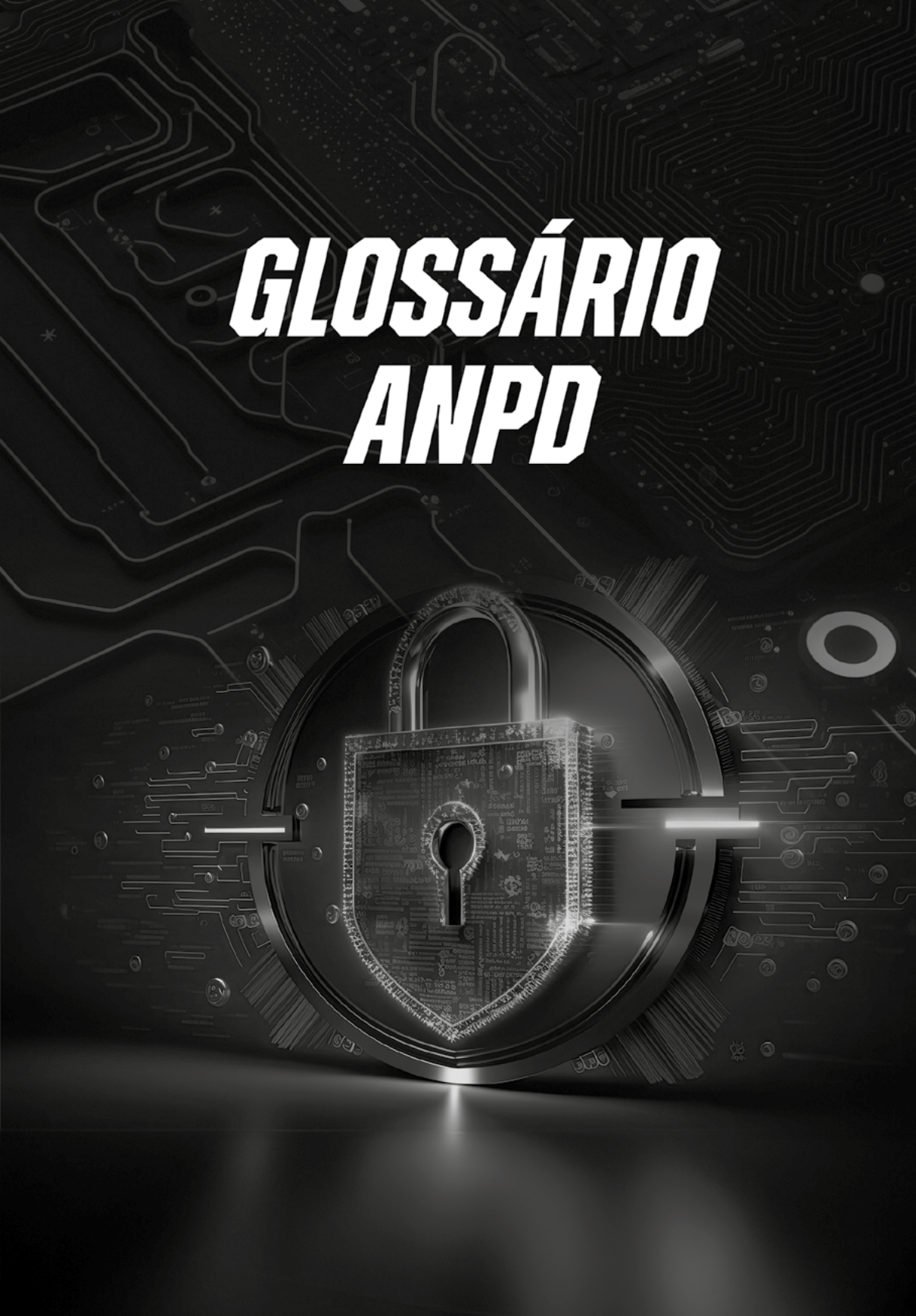
disponível em https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Acesso em: 19 abr. 2024.

GOV BR. Ministério da Justiça e Segurança Nacional. ANPD. Comunicação de Incidente de Segurança Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 20 abr. 2024.

PCSP. Guia de prevenção "Ransomware" (sequestro de dados). Disponível em https://www.policiacivil.sp.gov.br/portal/imagens/GUIA%20RANSONWARE%20v2.pdf. Acesso em: 21 abr. 2024.

SUPERGOV.BR. Sistema Único de Processo Eletrônico em Rede. Disponível em: https://super.presidencia.gov.br/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_gerar_senha&id_orgao_acesso_externo=0. Acesso em 21 abr. 2024.

GLOSSÁRIO ANPD



Recortes importantes e seus significados:

- **Agentes de Tratamento:** Controlador e operador responsáveis pelo tratamento de dados pessoais.
- **Agentes de Tratamento de Pequeno Porte:** Microempresas, empresas de pequeno porte e startups com menor potencial ofensivo aos direitos dos titulares.
- **Agentes Regulados**: Entidades sujeitas à regulação da ANPD.
- **ANPD - Autoridade Nacional de Proteção de Dados:** Órgão responsável por zelar pela proteção de dados pessoais no Brasil.
- **Aviso de Privacidade:** Documento que descreve como uma organização coleta, usa e protege os dados pessoais dos usuários.
- **Banco de Dados:** Conjunto estruturado de dados pessoais.
- **Banners de Cookies:** Ferramentas para informar e obter consentimento sobre o uso de cookies.
- **Consentimento:** Manifestação livre, informada e inequívoca do titular concordando com o tratamento de seus dados.
- **Controlador:** Pessoa ou entidade responsável pelas decisões sobre o tratamento de dados pessoais.
- **Controladoria Conjunta:** Situação onde dois ou mais controladores determinam conjuntamente os objetivos e meios de tratamento.
- **Controle de Acesso:** Mecanismos para restringir o acesso a dados pessoais.
- **Cookies:** Arquivos armazenados no dispositivo do usuário para diversas finalidades, incluindo análise de desempenho e publicidade.

- **Dado Anonimizado:** Dado que não pode ser associado a um indivíduo específico após a anonimização.

- **Dado Pessoal:** Informação relacionada a pessoa natural identificada ou identificável.

- **Dado Pessoal Sensível:** Dados sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, etc.

- **Eliminação:** Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

- **Encarregado:** Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

- **Finalidade:** Objetivo específico para o qual os dados pessoais são tratados.

- **Fiscalização:** Atividades de monitoramento, orientação e atuação preventiva, conforme os procedimentos previstos na Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

- **Grau do dano:** Extensão do dano e o prejuízo causado, nos termos do art. 54 da LGPD.

- **Grupos Afetados:** Categorias de agentes de tratamento e de titulares que podem ser mais impactadas pelos efeitos de determinada Ação de Normatização.

- **Incidente de Segurança:** Evento que compromete a segurança dos dados pessoais.

- **Legítima Expectativa:** É a expectativa razoável do titular, que deve ser demonstrada pelo controlador, de que o tratamento de

dados pessoais, para a finalidade pretendida, é o esperado em determinada situação concreta.

- **Legítimo Interesse:** Base legal para o tratamento de dados pessoais quando necessário para atender interesses legítimos do controlador ou terceiros.

- **Lei Geral de Proteção de Dados Pessoais (LGPD):** Lei que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

- **Medidas de segurança, técnicas e administrativas:** Medidas 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.

- **Microempresas e Empresas de Pequeno Porte:** Sociedade empresária, sociedade simples, sociedade limitada unipessoal, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e 18-A, §1º da Lei Complementar nº 123, de 14 de dezembro de 2006.

- **Operador:** Pessoa ou entidade que realiza o tratamento de dados pessoais em nome do controlador.

- **Política de Cookies:** Declaração que informa sobre o uso de cookies em um site ou aplicativo.

- **Política de Segurança da Informação – PSI:** Conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização.

- **Princípio da Adequação:** Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

- **Princípio da Finalidade:** Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

- **Princípio da Não Discriminação:** Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

- **Princípio da Necessidade:** Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

- **Princípio da Prevenção:** Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

- **Princípio da Qualidade dos Dados:** Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

- **Princípio da Responsabilização e Prestação de Contas:** Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

- **Princípio da Segurança:** Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

- **Princípio da Transparência:** Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

- **Princípio do Livre Acesso:** Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

- **Programa de Governança em Privacidade (PGP):** Instrumento capaz de demonstrar a integridade e o comprometimento do agente de tratamento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais. Nesse sentido, cabe destacar alguns processos e políticas importantes para a governança dos dados pessoais.

- **Pseudonimização:** Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

- **Ramo de Atividade Empresarial:** Área de atuação de empresa, grupo ou conglomerado de empresas, conforme definido pela ANPD e verificado no caso concreto, podendo ser comprovada mediante objeto social, código de Classificação Nacional de Atividades Econômicas (CNAE), código de serviço diretamente relacionado, ou instrumentos congêneres.

- **Relatório de Análise de Impacto Regulatório (AIR):** Ato de encerramento da Análise de Impacto Regulatório (AIR), que deve conter os elementos que subsidiaram a escolha da alternativa mais adequada ao enfrentamento do problema regulatório identificado e, se for o caso, a minuta do ato normativo a ser editado.

- **Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

- **Suboperador:** Contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.

- **Teste de Balanceamento:** Avaliação de proporcionalidade realizada pelo controlador com base no contexto e nas circunstâncias específicas do tratamento de dados, levando em consideração os impactos e os riscos aos direitos e liberdades dos titulares.

- **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- **Transferência Internacional de Dados:** Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

- **Tratamento:** Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

- **Tratamento de Dados Pessoais de Alto Risco:** Tratamento de dados pessoais que atende cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:

  Critérios gerais:

  a. tratamento de dados pessoais em larga escala; ou
  b. tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;

  Critérios específicos:

  a. uso de tecnologias emergentes ou inovadoras;
  b. vigilância ou controle de zonas acessíveis ao público;
  c. decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
  d. utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

- **Tratamento de Dados Pessoais em Larga Escala:** Tratamento de dados pessoais que abrange número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado.

- **Tratamento de Dados Pessoais que Possa Afetar Significativamente Interesses e Direitos Fundamentais dos Titulares:** Aquele em que a atividade de tratamento possa impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

- **Uso Compartilhado de Dados:** Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

GLOSSÁRIO ANPD. Esses termos e definições são extraídos do Glossário de Proteção de Dados Pessoais e Privacidade da ANPD【7:0†ANPD. Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd. Acesso em: 15jun. 2024.