IGOR DE CASTRO CARVALHO

LGPD E PODER PÚBLICO: A NECESSIDADE DE PROFISSIONAIS DPO NA ADMINISTRAÇÃO PÚBLICA

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO
Uberlândia – MG
2022

IGOR DE CASTRO CARVALHO

LGPD E PODER PÚBLICO: A NECESSIDADE DE PROFISSIONAIS DPO NA ADMINISTRAÇÃO PÚBLICA

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Federal de Uberlândia, como requisito para a obtenção do título de Bacharel em Direito.

Orientador: Prof. *Dr. Luiz Carlos Figueira de Melo*

Uberlândia - MG

2022

FICHA DE APROVAÇÃO

IGOR DE CASTRO CARVALHO

LGPD E PODER PÚBLICO: A NECESSIDADE DE PROFISSIONAIS DPO NA ADMINISTRAÇÃO PÚBLICA

Trabalho de Conclusão de Curso aprovado para a obtenção do título de Bacharel no Curso de Graduação em Direito da Universidade Federal de Uberlândia (UFU) pela banca examinadora formada por:

Uberlândia, ____ de _____ de 2023.

_____

Prof. Dr. Luiz Carlos Figueira de Melo

_____

Prof. Dr. Almir Garcia Fernandes

_____

Mestrando pós-graduado Erick Hitoshi Guimarães Makiya

RESUMO

Desde que as ferramentas digitais passaram a fazer parte do cotidiano dos brasileiros, uma série de mudanças aconteceu nas relações de consumo e nas próprias relações sociais. Com o desenvolvimento da *internet*, se tornou muito mais fácil a comunicação entre parentes distantes e a compra de produtos de regiões distintas. Ocorre que, neste mundo digital, o volume de dados que é transitado nesta rede de relações é gigantesco, e o potencial de dano causado por uma operação ruim destes dados também. O mundo está se transformando, o setor privado está reconhecendo esta mudança e se atualizando, cabe, então, à Administração Pública, ter também um bom reconhecimento destas transformações, e abrir espaço para que profissionais especialistas em proteção de dados – chamados de profissionais DPO – façam parte de seu corpo de trabalho. Nesta perspectiva, o estudo demonstra como o trabalho dos profissionais DPO, é necessário para a eficiência da Administração Pública, através de análise hermenêutica da legislação e de casos práticos.

Palavras-chaves: ferramentas digitais; Administração Pública; proteção de dados; profissionais DPO.

ABSTRACT

Since digital tools became part of Brazilians' daily lives, a series of changes have occurred in consumer relations and social relationships themselves. With the development of the internet, it has become much easier to communicate with distant relatives and buy products from different regions. However, in this digital world, the volume of data that is transmitted in this network of relationships is enormous, and the potential for damage caused by poor data management is also significant. The world is changing, and the private sector is recognizing this change and updating itself. It is up to the Public Administration to also recognize these transformations and make room for data protection specialists, called DPO professionals, to be part of their workforce. In this perspective, the study demonstrates how the work of DPO professionals is necessary for the efficiency of the Public Administration, through hermeneutic analysis of legislation and practical cases.

Keywords: digital tools; Public Administration; data protection; DPO professionals.

SUMÁRIO

1 INTRODUÇÃO

No contexto mundial atual muito se fala em tecnologia, automatização, realidade virtual, inteligência artificial e evolução tecnológica. De fato, quando se observa as atividades realizadas pelas pessoas no cotidiano, notam-se drásticas mudanças quando comparadas àquelas realizadas durante o início do milênio, nos anos 2000.

Os jornais impressos foram trocados pelos portais de notícias *on-line*, as caixas de correspondências trocadas pelos e-mails, as brincadeiras com bola de gude pelos vídeo games, e parte dos centros de convivências pelas redes sociais. Diante de tantas mudanças práticas, as áreas de conhecimento vão se atualizando de modo a compreender esta nova realidade.

Afinal, não se tratam apenas de mudanças, se mantém a necessidade dos cidadãos entenderem quais são os seus direitos e deveres, terem respeito pelo próximo e agirem de modo a sustentar uma boa convivência. O advento da tecnologia causou grande mudança na interpretação das relações jurídicas, mas não mudou os fundamentos que as criam.

Dignidade da pessoa humana, boa-fé, direito à propriedade, segurança e liberdade são princípios necessários para toda forma de relação social harmoniosa. O Poder Público necessita garantir o pleno cumprimento destes princípios, no relativo à sua competência, para que todo o País possa se desenvolver de forma saudável.

O Direito, por sua vez, sempre foi uma ferramenta utilizada pelos governantes para o desenvolvimento daquilo que governam, ou seja, o país. É através do Direito que se repreende determinadas condutas, e se promove outras de modo enfático.

Falar em Direito Digital, então, é falar em compreender a realidade atual. Os indivíduos sempre produziram dados sobre si mesmos, mas com a utilização cada vez maior de meios tecnológicos, tais dados são produzidos em maior quantidade e são colocados face à face a um novo perigo: os ataques digitais.

Desta forma, o Poder Público, nele compreendido todo agente e função que formam relações públicas, deve se atentar às mudanças provocadas pela tecnologia a fim de proteger os cidadãos e empoderar o desenvolvimento nacional. Com este cenário surge de forma urgente a necessidade da Administração Pública gerar cargos inteiramente voltados para a proteção de dados, sendo estes ocupados pelos profissionais até então chamados de *Data Protection Officer*, ou profissionais DPO.

Sendo assim, este trabalho tem como objetivo analisar a eficiência da Administração Pública na gestão de dados, com foco em como a atuação dos profissionais DPO pode ser benéfica para o Poder Público. O problema da pesquisa reside na operação inadequada dos dados que circulam na rede de relações sociais, o que pode causar danos enormes devido ao grande volume de informações envolvidas.

Para alcançar o objetivo proposto, foram traçados três objetivos específicos: entender como a eficiência da Administração Pública pode ser aprimorada na tarefa de gerenciar dados de forma adequada, analisar o papel dos profissionais DPO e apresentar sugestões para integrar os serviços destes profissionais, às necessidades da Administração Pública, considerando as mudanças trazidas pela era digital.

Visando o desenvolvimento da pesquisa, foi utilizada a metodologia de investigação cuidadosa da legislação e de casos práticos por meio de análise hermenêutica. Assim, foi viável conduzir uma pesquisa minuciosa sobre o assunto e reunir informações significativas para o estudo em questão.

Em suma, este trabalho tem como objetivo contribuir para o aprimoramento da gestão de dados na Administração Pública, a partir da compreensão do papel dos profissionais DPO e da sugestão de estratégia para integrar seus serviços às necessidades da era digital. A metodologia utilizada buscou garantir uma análise fundamentada e cuidadosa do tema, a fim de fornecer conclusões relevantes para a discussão.

2 A INTRODUÇÃO EXPRESSA DA PROTEÇÃO DE DADOS PESSOAIS NA CONSTITUIÇÃO FEDERAL

Quando se fala em proteção de dados pessoais no Brasil a primeira legislação que é lembrada é a Lei Geral de Proteção de Dados Pessoais, também chamada de LGPD, sendo ela a lei 13.709, de 14 de agosto de 2018. De fato, é o dispositivo legal que direcionou uma atenção necessária para a proteção de dados pessoais no Brasil, visto que normativas anteriores não eram suficientes para abordar o tema.

Ocorre que, com a promulgação da LGPD, ficou ainda mais claro que a proteção de dados pessoais é um direito essencial de todo indivíduo, que deve ser respeitado para que se preserva a sua dignidade. Com a LGPD, ficou ainda mais evidente que todos os cidadãos correm o risco de terem seus dados expostos de forma indevida.

Com isto, a Emenda Constitucional nº 115, de 2022, garantiu à proteção dos dados pessoais o caráter de direito fundamental, de forma expressa. O texto do dispositivo legal inserido através da citada emenda no artigo 5º, da Constituição Federal (CF) (BRASIL, [2016]), determina que a lei garante à todos a proteção dos dados pessoais.[1]

Nota-se, também, que o texto legal abordou de forma expressa os termos meios digitais. Isto é interessante, pois foi justamente o surgimento dos meios digitais de relações sociais, que evidenciou a necessidade de proteção dos dados pessoais, como veremos a seguir.

---

[1]BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 17 de dezembro de 2022. Art. 5º, inciso LXXIX: “Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[…]

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

3 A CIRCULAÇÃO DE DADOS NO MUNDO CONTEMPORÂNEO

Direito Fundamental é, no geral, entendido como aquilo que não pode ser violado para que se tenha dignidade, paz e harmonia social. Apesar do Poder Judiciário brasileiro constantemente enxergar possibilidade de se limitar direitos fundamentais por meio do chamado sopesamento, é de consenso que aquilo que é fundamental no âmbito do direito são as bases que ordenam todo o sistema jurídico, de modo a sustentar todo o conhecimento científico que se têm produzido na área.

Observa-se, também, que o Direito é um tipo de ferramenta que garante o livre exercício destes direitos fundamentais, em especial se observada a Constituição Federal. Nela, estão inscritos muitos direitos fundamentais com a garantia expressa de serem invioláveis, podendo ser citado: direito à vida, liberdade, igualdade, segurança e propriedade.

Ao se analisar o modo que as pessoas se relacionam atualmente por intermédio da *internet*, é possível notar que na prática aconteceu uma grande transformação no modo de conviver das pessoas, mas não necessariamente uma origem, inicialização, de direitos que não existiam. É com esta linha do pensamento que foi adotado, no artigo 5º da Constituição Federal brasileira (CF), a expressão “direito à proteção dos dados pessoais”.

Em tempos remotos, quando uma pessoa se dirigia a uma farmácia para comprar um remédio, ela não tinha que oferecer dados como CPF, RG e profissão. Entretanto, estes dados sempre foram dela, relativos à sua existência no meio jurídico e social.

A realidade atual se mostra bem diferente. É comum que um cidadão, ao comprar um remédio, seja perguntado sobre seu nome, idade e profissão. Isto pode acontecer por diversos motivos, entre eles comerciais (de modo que a farmácia, ao saber mais sobre o consumidor, consegue oferecer produtos mais atrativos para este) e de saúde pública (o Governo, ao conhecer de modo preciso como está a saúde pública de seus administrados, consegue destinar de forma mais precisa recursos materiais e humanos).

Mas o que acontece se a base de dados da farmácia, composta pelas fichas

cadastrais de seus clientes, for violada por meio de um ataque hacker? O que acontece se um funcionário desta farmácia não tiver sido bem treinado e, ao invés de lançar os dados dos clientes na plataforma interna da empresa, lançar eles num perfil aberto em uma rede social? E se o diretor da farmácia em busca de lucro, vender fichas com os dados dos seus clientes para empresas parceiras de seu negócio?

A resposta é simples, se tem um direito fundamental violado. E as consequências disto são inúmeras, afinal, um terceiro que tenha posse não autorizada dos dados de outras pessoas pode buscar fraudar o sistema de benefícios do INSS, ou realizar compras utilizando patrimônio que não é seu, ou até mesmo criar perfis falsos em redes sociais para denegrir a imagem outrem.

Não há uma limitação às áreas potenciais de dano que podem ser afetadas com um uso de dados não autorizado. O verdadeiro titular dos dados pode sofrer dano financeiro, à sua reputação social, à sua carreira profissional, à sua autoestima, à sua liberdade de locomoção, entre vários outros.

4 O CARÁTER FUNDAMENTAL DA PROTEÇÃO DE DADOS

Segundo Guimarães e Lecio Machado, a Lei Geral de Proteção de Dados Pessoais (LGPD):

> é uma legislação de grande importância e necessidade, pois visa efetivar garantias constitucionais da liberdade e da privacidade e o livre desenvolvimento da personalidade da pessoa natural nas relações entre pessoas físicas e jurídicas, de direito público ou privado, em relação a proteção de dados pessoais (...).[2]

[2]GUIMARÃES, João Alexandre; MACHADO, Lécio Silva. **Comentários à Lei Geral de Proteção de Dados: lei 13.709/2018 com alterações da MPV 869/2020**. 1. ed. Rio de Janeiro - RJ: Lumen Iuris, 2020. Pág. 01.

Vale ressaltar que, ainda antes da promulgação da LGPD, já existiam dispositivos legais que garantiam a proteção de dados pessoais em situações específicas. Isto, pois a proteção de dados pessoais é uma necessidade para garantir a dignidade do titular destes dados, e portanto um direito fundamental que, embora tenha se tornado expresso na Constituição Federal apenas recentemente, já era defendido por meio de normas que visavam garantir uma plena garantia dos princípios fundamentais.

Pode-se citar, de normas que versaram sobre a proteção de dados pessoais, de modo direto ou indireto, antes do surgimento da LGPD: artigos 43, 72 e 73 do Código de Defesa do Consumidor; artigo 4º, VII do Decreto do Comércio Eletrônico; os artigos 3º, III; 7º, VII, IX, X; 10; 11; 16, II do Marco Civil da Internet; o Capítulo IV, Seção V da Lei de Acesso a Informações e o Capítulo III do Decreto 8.771/16.

Mas existem diferenças claras entre as legislações citadas. Em 2015, o até então Ministro da Justiça, José Eduardo Cardozo, comparou o Marco Civil da Internet com a Lei Geral de Proteção de Dados Pessoais, a qual ainda era um projeto de lei, e disse:

> A realidade da proteção de dados pessoais é a mesma do Marco Civil da Internet, mas são assuntos com enfoques diferentes. No Marco Civil da Internet nós temos as relações disciplinadas no plano da internet; no outro o que se protege é o dado da pessoa e suas referências pessoais. É claro que tem um ponto de ligação. Por exemplo, os dados pessoais que você tem cadastrados numa loja podem ser passados para alguém ou negociados? Os dados do governo podem ser cedidos? Esse é o enfoque do projeto[3]

No relativo à proteção principiológica que o reconhecimento da proteção de dados pessoais como direito fundamental proporciona, observa-se que tal proteção se origina dos próprios conceitos de proteção de dados e segurança da informação. Ann Cavoukian desenvolveu, no Canadá, o conceito de *privacy by design*, conhecido

---

[3]BRASIL, Emanuelle e ASSUMPÇÃO, Regina Céli. Consulta pública será base para projeto de lei sobre proteção de dados pessoais. **Agência Câmara de Notícias**, 28 de janeiro de 2015. Disponível em: < https://www.camara.leg.br/noticias/449278-consulta-publica-sera-base-para-projeto-de-lei-sobre-protecao-de-dados-pessoais/ >. Acesso em: 15 de dezembro de 2022.

no Brasil como “A privacidade por concepção”.

Tal modelo estabelece que a privacidade dos dados pessoais deve ocorrer desde o momento da coleta destes dados, e que deve acontecer mediante a aplicação de sete princípios: Privacidade por padrão ou *privacy by default*; Princípio da funcionalidade completa; Princípio da segurança de ponta a ponta; Proatividade; Privacidade incorporada ao *design*; Visibilidade e transparência e Respeito à privacidade do usuário.

Carloto, Bramante e Cavalini (2022, p.137 - p.139), definiram tais princípios de forma objetiva e completa, sendo o princípio da privacidade por padrão aquele que diz respeito à ideia de limitação, de modo que, desde a coleta até o descarte dos dados, estes devem ser usados apenas para a finalidade ou propósito específico pelo qual foram utilizados. É o pensamento de garantir uma segurança por padrão.

Já o princípio da funcionalidade completa é relativo ao funcionamento completo de um bom sistema de proteção de dados pessoais, de modo que as ferramentas utilizadas e as áreas de conhecimento aplicadas estejam em completa harmonia para que não haja falhas de segurança. É a ideia de segurança realmente aliada à privacidade durante todo o uso de dados.

O princípio da segurança ponta a ponta, por sua vez, condiz com a ideia de que a proteção deve estar presente e ser utilizada de forma adequada durante todo o ciclo de vida do dado a ser utilizado. É este princípio que assegura, também, a necessidade de destruição dos dados após a finalização de sua utilização.

Enquanto o princípio da proatividade determina que devem ser tomadas medidas proativas e reativas à utilização de dados pessoais, visando prever possíveis situações de violação de acesso à dados pessoais e promover medidas efetivas para evitá-las. Consiste no pensamento de que deve haver uma proteção de todo dado privado, esteja este em vulnerabilidade ou não.

Já o conceito de privacidade incorporada ao *design* é a ideia de que a privacidade não é um aditivo para os sistemas computadorizados e para os negócios realizados. É um elemento intrínseco, essencial, para o bom funcionamento das ferramentas digitais e das prestações de serviço.

Neste âmbito, os princípios da visibilidade e transparência dizem respeito à

condutas que o operador de dados deve possuir. Sua atitude deve acontecer sem utilizar de omissão em relação ao titular dos dados.

Por último, o princípio do respeito à privacidade do usuário condiz com o pensamento de que a privacidade deve ser um grande foco do operador de dados, já que é de grande interesse do titular destes dados. É este princípio que determina, também, a constante atualização sobre as ferramentas de proteção de dados no âmbito da segurança da informação[4].

Os princípios citados demonstram como a proteção de dados aborda questões fundamentais para a área da Segurança da Informação, e acaba por "escancarar" como o reconhecimento de tal proteção como direito fundamental só tem a agregar na compreensão clara das relações sociais. A garantia de cada indivíduo ter a proteção de seus dados é tão importante, que seu reconhecimento transcende a área do Direito propriamente dito.

5 A INTEGRAÇÃO ENTRE O PROFISSIONAL DPO E A PROTEÇÃO DE DADOS

De maneira sintética, o profissional DPO é aquele trabalhador encarregado de garantir que a proteção de dados está acontecendo dentro de um sistema. Como grande parte dos sistemas utilizados pelas organizações são digitais, é de consenso que quem exerce tal função, tenha conhecimento tanto de Direito quanto de Tecnologia – seja na área de Sistemas da Informação, Ciência da Computação, Engenharia de *Software* ou similares.

Carloto, Bramante e Cavalini (2022, p.57) definem as atribuições do profissional DPO como: Aceitar reclamações e comunicações dos titulares; Prestar esclarecimentos e adotar providências; Receber comunicações da Autoridade Nacional de Proteção de Dados – ANPD, e adotar providências; Orientar os funcionários e os contratados da empresa a respeito das práticas a serem tomadas

[4]CARLOTO, Selma; BRAMANTE, Ivani Contini; CAVALINI, Juliane Pascoeto. **Lei Geral da Proteção de Dados e Segurança da Informação: Perguntas e Respostas**. 1. ed. LTr, 2022.

em relação à proteção de dados pessoais; Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.[5]

É importante ressaltar que o profissional DPO faz uma ponte de comunicação entre o titular dos dados e a organização que está gerindo estes dados, de modo que pode ser exigido dele tanto questões técnicas como aprimoramento de sistema de *software* (ou programa) de proteção de dados, ou conhecimento de dispositivos legais sobre proteção de dados, quanto assuntos de relacionamento pessoal, podendo se exemplificar o recebimento de reclamações ou sugestões.

Por fim, mister pontuar a importância do profissional DPO perante a Autoridade Nacional de Proteção de Dados (ANPD). A ANPD é um órgão da Administração Pública que tem todo o seu trabalho voltado para a efetiva aplicação da Lei Geral de Proteção de Dados Pessoais, em todo o Brasil.

Com funcionamento efetivo desde 05 de novembro de 2020, a ANPD precisa de comunicadores que trabalhem em todo o território nacional para que se tenha uma efetiva garantia de proteção de dados pessoais nas organizações. É necessário a figura de um especialista que entenda o conhecimento teórico sobre a proteção de dados, e que saiba como aplicá-los perante as organizações e os cidadãos que dela utilizem. Nisto, entra o trabalho do profissional DPO.

6 COMO A PROTEÇÃO DE DADOS PESSOAIS ACONTECE NO SETOR PRIVADO

Para entender a prática da aplicação dos princípios que envolvem a proteção de dados pessoais, é interessante observar como as organizações têm se movimentado para realizar as operações com dados de forma legal. O setor privado, que constantemente se regula de acordo com a própria movimentação de mercado, é um ambiente no qual o conhecimento teórico sobre proteção de dados, tem sido muito aplicado no cotidiano.

---

[5]CARLOTO, Selma; BRAMANTE, Ivani Contini; CAVALINI, Juliane Pascoeto. **Lei Geral da Proteção de Dados e Segurança da Informação: Perguntas e Respostas**. 1. ed. LTr, 2022. Pág. 57.

Se mostra interessante, por exemplo, o modo como são destruídas as mídias que não são mais utilizadas por uma empresa, já que o descarte de mídias pelas organizações requer uma atenção especial. Sendo uma mídia com informação confidencial, seu descarte deve acontecer de forma segura e protegida, e é comum, quando uma mídia possui informações confidenciais e informações não confidenciais, o descarte de toda a mídia, pois a identificação e separação dos conteúdos confidenciais pode ser mais trabalhosa.

Esta eliminação pode acontecer por incineração, fragmentação ou trituração, e existem empresas que prestam o serviço de descarte seguro destes itens. Ademais, como lembram Carloto, Bramante e Cavalini (2022, p.141): “O descarte de itens sensíveis deverá ser registrado para se manter trilha de auditoria, nos termos da ISO 27002”.[6]

Importante entender as etapas de tratamento de dados pessoais pois está bem claro que a tecnologia faz parte do cotidiano das pessoas, e é bem evidente que os meios tecnológicos terão ainda mais uso no futuro. Pautas como criptomoedas, automatização de tarefas administrativas, jurimetria, utilização de inteligência artificial e influenciadores digitais estão cada vez mais presente nos portais noticiários.

É evidente, também, que a tecnologia será mais utilizada não só nas relações pessoais, mas também nos meios profissionais. No novo milênio, os próprios processos jurídicos passaram por uma grande transformação, sendo digitalizados aqueles que surgiram em meios físicos, e digitais aqueles que surgiram após a implementação do processo judiciário eletrônico.

Neste sentido, observa-se que existe tanto uma demanda pessoal quanto profissional por pessoas que são capazes de garantir a proteção dos dados pessoais que flutuam por estas plataformas digitais. Da mesma forma que o mundo digital traz consigo uma série de inovações e ânimo criativo, ele traz um espaço novo onde criminosos podem atuar se utilizando de uma suposta anonimidade.

---

[6]CARLOTO, Selma; BRAMANTE, Ivani Contini; CAVALINI, Juliane Pascoeto. **Lei Geral da Proteção de Dados e Segurança da Informação: Perguntas e Respostas**. 1. ed. LTr, 2022. Pág. 141.

Esta demanda ficou escancarada em uma pesquisa realizada pelo Serasa Experian, empresa que atua com serviços de informações para apoio na tomada de decisões das empresas. Após apurar a opinião de 508 executivos que lideram empresas de 18 ramos de atividade diferentes, com diversos capitais e locais de funcionamento, se constatou que 85% das empresas participantes da pesquisa, não estavam prontas para seguirem corretamente os limites estabelecidos pela Lei Geral de Proteção de Dados Pessoais[7].

Desta forma, faz-se necessário que sejam utilizadas áreas do conhecimento que já estão sendo estudadas na atualidade, para que aconteça uma implementação pacífica das ferramentas digitais. Assim, tanto o Direito quanto a Tecnologia da Informação, ambas áreas presentes nas Universidades e muito bem estudadas, se mostram as mais adequadas para aqueles que pretendem se desenvolver como um profissional de proteção de dados pessoais.

Exatamente por este motivo que os profissionais DPO são aqueles que advém de formação no Direito ou em alguns dos setores de conhecimento da Tecnologia da Informação, ou ainda de ambos. É fato que sua atividade gera necessidade de conhecimento das duas áreas: o profissional precisa entender quais são os limites para o uso de dados pessoais pelos grupos coletivos (sejam empresas ou o próprio Governo), e necessita compreender como tais grupos coletivos podem implementar e sustentar um sistema que não esteja facilmente sujeito ao vazamento de dados.

Para compreender melhor a complexidade do trabalho a ser realizado pelos profissionais DPO, no relativo ao âmbito do Direito, Patrícia Peck Pinheiro estabeleceu uma série de documentos que já existem no âmbito de grandes empresas e que precisam ser atualizados após a promulgação da Lei Geral de Proteção de Dados, sendo estes: mapa de fluxo de dados pessoais; Tabela de temporalidade de guarda de *logs* de consentimento; Política de gestão de dados pessoais; Política de tratamento de dados pessoais para terceirizados; Termo de uso

[7]85% DAS EMPRESAS DECLARAM QUE AINDA NÃO ESTÃO PRONTAS PARA ATENDER ÀS EXIGÊNCIAS DA LEI DE PROTEÇÃO DE DADOS PESSOAIS, MOSTRA PESQUISA DA SERASA EXPERIAN. **Serasa Experian**, 2019. Disponível em: < https://www.serasaexperian.com.br/sala-de-imprensa/estudos-e-pesquisas/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian/ >. Acesso em: 19 de dezembro de 2022.

e Política de privacidade; Contratos; NDA; *Check-list Compliance*; Código de Conduta e Política de Segurança da Informação (PINHEIRO, 2020)[8].

Daniel Donda, por sua vez, estabeleceu de modo sintético as ações técnicas a serem adotadas na implementação da LGPD em uma organização, sendo estas: Identificar o ciclo de vida de dados; Avaliar se é realmente necessário o armazenamento desses dados; Identificar e controlar os acessos; Mapear os controles de segurança aplicados na proteção dessas informações; Analisar o risco, identificar possíveis vulnerabilidades, determinar a probabilidade de uma ameaça e explorar uma vulnerabilidade existente; Monitorar o tratamento dos dados, quem está acessando e de onde, quais ações estão acontecendo, a fim de detectar atividades suspeitas ou acessos não autorizados, e manter o ambiente em conformidade (DONDA, 2020)[9].

Donda destaca, ainda, que uma boa política de informação abrange três diferentes níveis de aplicação: estratégico, tático e operacional. Mas, apesar destes conceitos remeterem ao âmbito da tecnologia da informação, ele relembra que o apoio jurídico para a implementação de um sistema de proteção de dados pessoais é importante e necessário (DONDA, 2020)[10]. Vale lembrar que tal atuação jurídica não se limita à um momento específico no qual o advogado dá seu parecer sobre como se adequar à norma, mas envolve, também, a revisão de documentos que eventualmente venham a ser exigidos por lei, a monitoração da proteção existente no ambiente de trabalho e a constante consultoria sobre assuntos que gerem dúvidas à organização.

É de se notar, também, que muitas vezes a aplicação de um sistema regular à Lei Geral de Proteção de Dados pode acontecer mediante análise de um contexto internacional, e não puramente interno. Isto acontece pois a Internet permite a comunicação e o comércio entre países de forma célere e eficiente, o que possibilita

---

[8]PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018**. 2. ed. São Paulo - SP: SaraivaJur, 2020. Pág. 66-67.

[9]DONDA, Daniel. **Guia Prático de Implementação da LGPD**. 1. ed. São Paulo - SP: Labrador, 2020. Pág. 31.

[10]DONDA, Daniel. **Guia Prático de Implementação da LGPD**. 1. ed. São Paulo - SP: Labrador, 2020.

que grande parte dos consumidores de uma empresa nacional, sejam estrangeiros. Daí, surge outra necessidade, que é a de profissionais especialistas em áreas como Direito Internacional.

Segundo a secretária nacional do Consumidor em 2015, Juliana Pereira:

> Estamos juntos com a Alemanha e a China que discutem os modelos de privacidade de dados pessoais. Independentemente da regulamentação, todo trabalho que é feito pelo governo já é reconhecido internacionalmente, por conta do respeito que se tem no Brasil ao monitoramento desse tema. Quando nós falamos de proteção de dados pessoais, não estamos falando de um universo fechado, estamos falando de uma questão que ultrapassa em muito o conceito de soberania das fronteiras[11].

Importante destacar, também, que não existe um modelo metódico específico para tratamento dos dados pessoais. O operador de dados observa a estrutura, escala e volume das operações com dados realizadas em sua organização, depois observa o grau de sensibilidade dos dados a serem tratados, bem como a probabilidade e gravidade de danos decorrentes de uma eventual violação destes dados, e então atua seguindo as determinações da Lei Geral de Proteção de Dados Pessoais.

Sobre o assunto, Carloto, Bramante e Cavalini destacam:

> Não existe uma regra específica. A LGPD dispõe que os sistemas utilizados para o tratamento de dados pessoais deverão ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, sobretudo os princípios gerais previstos na LGPD e demais normas setoriais.[12]

---

[11]BRASIL, Emanuelle e ASSUMPÇÃO, Regina Céli. Consulta pública será base para projeto de lei sobre proteção de dados pessoais. **Agência Câmara de Notícias**, 28 de janeiro de 2015. Disponível em: < https://www.camara.leg.br/noticias/449278-consulta-publica-sera-base-para-projeto-de-lei-sobre-protecao-de-dados-pessoais/ >. Acesso em: 15 de dezembro de 2022.

[12]CARLOTO, Selma; BRAMANTE, Ivani Contini; CAVALINI, Juliane Pascoeto. **Lei Geral da Proteção de Dados e Segurança da Informação: Perguntas e Respostas**. 1. ed. LTr, 2022. Pág.

Sendo assim, cada organização arquiteta sua estrutura de proteção de dados da forma que parece mais eficiente e adequada para seu sistema de negócio. De todo modo, não pode extrapolar os limites legais de utilização de dados pessoais, e deve se nortear pelas boas práticas e instruções existentes sobre a utilização de dados.

7 CASOS RELEVANTES

Um caso prático interessante de ser analisado quando se fala em vazamento de dados é o ocorrido com a empresa brasileira de comércio eletrônico de artigos esportivos Netshoes. O Inquérito Civil Público n º 08190.044813/18-44 investigava a situação da empresa que permitiu, em janeiro de 2018, que vazassem informações de 1.999.704 contas cadastradas no site de compras da empresa[13].

Foram comprometidos dados pessoais como nome, CPF, e-mail, data de nascimento e histórico de compras. A empresa firmou com o Ministério Público do Distrito Federal e Territórios (MPDFT) termo de ajustamento de conduta (TAC), o qual foi proposto pela Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do MPDFT.

As organizações acordaram no pagamento de indenização no valor de R$500 mil pela empresa Netshoes, a qual será recolhida mediante depósitos no Fundo de Defesa de Direitos Difusos (FDD). De acordo com o sítio eletrônico do Ministério Público do Distrito Federal e Territórios:

> a Netshoes também se compromete a implantar medidas adicionais ao seu Programa de Proteção de Dados, a realizar esforços de orientação de

---

122.

[13]BRASIL. Ministério Público do Distrito Federal e Territórios**. MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados**. [Brasília]: Ministério Público do Distrito Federal e Territórios, 05 de fevereiro de 2019. Disponível em: < https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados >. Acesso em: 16 de dezembro de 2022.

> consumidores, a aumentar o nível de conhecimento sobre os riscos cibernéticos e medidas de proteção de seus dados pessoais, por meio de campanha de conscientização, e a disseminar ao mercado as melhores práticas para privacidade e proteção de dados pessoais.[14]

Outro caso interessante relacionado à proteção dos dados pessoais aconteceu no Tribunal de Justiça do Estado de São Paulo, no julgamento do Recurso Inominado Cível nº 1003086-21.2021.8.26.0003[15]. Na situação, a consumidora Ana Maria Nishimura da Cruz, estava em litígio com a empresa Eletropaulo Metropolitana Eletricidade de São Paulo S.A., e pleiteou que fosse provido pedido de reforma de sentença para que fosse julgado procedente o pedido de indenização por danos morais.

Ana Maria alegou que a empresa ré vazou seus dados pessoais e que, através disso, recebeu muitas ligações e mensagens de terceiros. Como a primeira sentença não acolheu seu pedidos iniciais, entrou com o citado Recurso Inominado.

O entendimento da 4ª Turma Recursal Cível - Santo Amaro do Colégio Recursal - Santo Amaro, foi o de que é aplicável a LGPD no presente caso, por ter acontecido no território nacional e após 17/09/2020. Foi entendido, também, que houve comprovação que a empresa permitiu o vazamento dos dados: “nome, CPF, data de nascimento, idade, telefone fixo, telefone celular, e-mail, carga instalada, consumo estimado, tipo de instalação, leitura e endereço”.

Diante disso, a 4ª Turma Recursal Cível - Santo Amaro do Colégio Recursal -

---

[14]BRASIL. Ministério Público do Distrito Federal e Territórios**. MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados**. [Brasília]: Ministério Público do Distrito Federal e Territórios, 05 de fevereiro de 2019. Disponível em: < https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados >. Acesso em: 16 de dezembro de 2022.

[15]SÃO PAULO. Tribunal de Justiça. **Recurso Inominado Cível nº 1003086-21.2021.8.26.0003**. Recorrente: Ana Maria Nishimura da Cruz. Recorrido: Eletropaulo Metropolitana Eletricidade de São Paulo S/A. Relator: Juiz Carlos Eduardo Santos Pontes de Miranda (4ª Turma Recursal Cível). São Paulo, 25 de outubro de 2021. Disponível em: < https://jurisprudencia.s3.amazonaws.com/TJ-SP/attachments/TJ-SP_RI_10030862120218260003_921dc.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1671619144&Signature=v0emL%2BHnUs6PQzceiaJX2QHClQw%3D >. Acesso em: 21 de dezembro de 2022.

Santo Amaro deu provimento ao pleiteo de Ana Maria por Indenização no valor de R$ 5.000,00 (05 mil reais).

Tais casos expõe a importância que a LGPD tem para a proteção dos dados pessoais dos indivíduos, e funcionam como um alerta para as organizações que ainda não se adequaram à lei. Para o Poder Público, devem servir como ponto de atenção em relação ao grande volume de dados que são operados no funcionamento da Administração Pública.

8 NECESSIDADE DE PROTEÇÃO DE DADOS PESSOAIS NO SERVIÇO PÚBLICO

Neste ano de 2022 aconteceu um caso que demonstra que o serviço público não está isento do perigo de violação de dados. O Banco Central do Brasil comunicou que, em relação ao cadastro de chaves PIX, informações como número da agência e contas bancárias, CPF, nome completo, e instituição, ligados à 160.147 chaves foram potencialmente expostos de maneira indevida.

A situação aconteceu entre 03 e 05 de dezembro de 2021. Os dados em questão estavam sob guarda e responsabilidade da empresa Acesso Soluções de Pagamento, mas, mesmo com o envolvimento da empresa privada, o caso demonstrou como a operação de dados no serviço público deve ser bem protegida.[16]

Outro caso que mostra o perigo do vazamento de dados no serviço público, aconteceu com o Ministério da Saúde. O órgão público foi notificado, em junho de 2020, pela Open Knowledge Brasil (OKBR), uma Organização da Sociedade Civil (OSC) sem fins lucrativos, sobre uma falha de segurança que permitia o vazamento de dados[17].

---

[16]ARAGÃO, Alexandre. 5 grandes vazamentos de dados no Brasil – e suas consequências. **Jota**, São Paulo, 28 de janeiro de 2022. Disponível em: < https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022 >. Acesso em: 16 de dezembro de 2022.

[17]CAMBRICOLI, Fabiana. Ministério da Saúde foi alertado em junho por ONG sobre outra exposição indevida de dados. **O Estado de São Paulo**, 27 de novembro de 2020. Disponível em: <

Posteriormente, a equipe da reportagem do jornal O Estado de São Paulo revelou que, por falha do sistema de segurança do Ministério da Saúde, dados de 243 milhões de brasileiros ficaram expostos na internet. Pelo período de seis meses, o erro permitiu o acesso a dados pessoais de todos os brasileiros cadastrados no SUS e clientes de plano de saúde [18].

Neste caso do Ministério da Saúde, uma vulnerabilidade do código do Ministério permitia que qualquer pessoa consultasse o banco de dados da organização e tivesse acesso à informações como endereço, telefone, CPF e nome completo. Tais informações deveriam estar protegidas por login e senha.

E pode-se citar, também, o caso da empresa Enel, de 2020. A empresa Enel é uma multinacional que atua no ramo de geração e distribuição de eletricidade e gás. Atualmente a organização é uma Sociedade Anônima, mas foi estabelecida no Brasil como Entidade Pública em 1962.

Cerca de 290 mil clientes da Enel em Osasco, São Paulo, tiveram dados sensíveis vazados por falha de segurança da empresa. Foram expostos dados cadastrais, históricos de pagamentos, índices de leitura e nível de consumo[19].

Os casos citados demonstram de forma prática que a Administração Pública precisa ter um sistema robusto de segurança da informação, que não permita que ocorram violações de acesso à dados.

9 CAMINHO A SER TRAÇADO

De início, ressalta-se que os envolvidos na elaboração da Lei Geral de

---

https://www.estadao.com.br/saude/ong-alertou-ministerio-em-junho-que-dados-de-pacientes-eram-vulneraveis/ >. Acesso em: 21 de dezembro de 2022.

[18]CAMBRICOLI, Fabiana. Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. **O Estado de São Paulo**, 02 de dezembro de 2020. Disponível em: < https://www.estadao.com.br/saude/nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes/ >. Acesso em: 21 de dezembro de 2022.

[19]ARAGÃO, Alexandre. 5 grandes vazamentos de dados no Brasil – e suas consequências. **Jota**, São Paulo, 28 de janeiro de 2022. Disponível em: < https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022 >. Acesso em: 16 de dezembro de 2022.

Proteção de Dados Pessoais sabiam da importância que esta lei teria para o serviço público. Isto, pois é evidente que se existe a necessidade de empresas privadas terem um zelo pelos dados de seus consumidores, o Poder Público também deve ter este zelo com seus administrados.

Quando se fala em serviço público, ainda, a importância da proteção de dados pessoais se torna maior, uma vez que no serviço público dados íntimos dos indivíduos (como processos em segredo de justiça, declaração de renda e histórico médico) são constantemente trabalhados. Então, a principal legislação sobre a proteção de dados pessoais, no Brasil, é certeira quando dedica um espaço próprio para dispor sobre o serviço público.

Este espaço é o Capítulo IV da Lei citada, o qual é intitulado “Do tratamento de dados pessoais pelo Poder Público”, e é dividido em duas seções: Seção I – Das Regras e Seção II – Da Responsabilidade. O legislador acerta, também, ao dedicar uma seção específica para falar sobre a responsabilidade, pois a quantidade de dados pessoais que são operados pelo Poder Público, justificam um enfoque especial sobre a responsabilidade do Estado.

Destarte, acentua-se dois artigos do capítulo citado: o artigo 29 e o artigo 23, inciso III. O artigo 29 dá poderes para a autoridade nacional emitir parecer técnico complementar, solicitar realização de operações de tratamento de dados pessoais, além de informações específicas sobre a área e natureza dos dados que estão sendo tratados, e também detalhes deste tratamento, às entidades e órgãos do poder público.[20]

Este dispositivo demonstra como a atuação da ANPD no cenário nacional é ampla e de extrema relevância nos órgãos e entidades do serviço público. Como a ANPD tem a prerrogativa de solicitar, a qualquer momento, operações de tratamento de dados pessoais, informações e detalhes, se presume que os órgãos e entidades do serviço público devem ser dotados de recurso de pessoal com conhecimento e

---

[20]Lei Geral de Proteção de Dados Pessoais (**LGPD**). Brasília, DF: Presidência da República, [2020]. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. >. Acesso em: 19 de dezembro de 2022. “Art. 29: A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei”.

habilidade suficientes para suprir às exigências da ANPD.

Neste caso, as solicitações da ANPD servem para cumprir o que está disposto na Lei Geral de Proteção de Dados Pessoais e devem ser observadas como medidas necessárias para garantir a eficácia da Administração Pública. Se o Poder Público não dispor de corpo técnico suficiente para garantir um robusto sistema de proteção de dados e de transparência sobre o uso destes dados, os lesados de forma direta são os próprios administrados.

Já o artigo 23, inciso III, expressa que é necessário que haja indicação de um encarregado nas situações em que pessoas jurídicas de direito público realizarem operações de tratamento de dados pessoais, além de que estas operações só podem ser realizadas quando se tem uma finalidade pública, nos moldes da existência de interesse público, para que sejam cumpridas competências ou atribuições legais do serviço público.[21]

Esta norma legal deixa claro, então, que já existe previsão legal para a atuação do profissional DPO na Administração Pública. O próprio texto da lei determina a indicação de um encarregado para o tratamento de dados pessoais pelas pessoas jurídicas de direito público.

Quando se analisa o art. 1º da Lei nº 12.527/2011 (Lei de Acesso à Informação), seu parágrafo único e incisos I e II, acabam por demonstrar que a atuação do encarregado de proteção de dados no Serviço Público se dará tanto no âmbito da Administração Direta quanto da Administração Indireta, já que referido dispositivo legal determina o âmbito de atuação nos órgãos públicos que fazem parte da Administração Direta - incluindo as Cortes de Contas e o Ministério Público - e outras entidades que estão sob controle direto ou indireto da União, Estados, Distrito

---

[21]Lei Geral de Proteção de Dados Pessoais (**LGPD**). Brasília, DF: Presidência da República, [2020]. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. >. Acesso em: 19 de dezembro de 2022. “Art. 23, inciso III: O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

[…]

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e”.

Federal e Municípios.[22]

Inegável, então, que o próprio legislador já reconheceu a necessidade do profissional DPO na Administração Pública, e se mostra lógico, a partir da pesquisa desempenhada neste trabalho e no contexto tecnológico atual, que este encarregado seja um agente público, que trabalhe com foco em suprir as necessidades da Administração Pública.

Se mostra lógico, também, que tal profissional tenha conhecimento nas áreas de Direito e nas áreas de conhecimento que abordam o mundo da tecnologia, como aqui já defendido. O profissional DPO, então, poderia ter seu ingresso na Administração Pública para ocupar um cargo nomeado como Profissional DPO, cuja principal atribuição seja exercer o papel do encarregado de tratamento de dados", suprindo as solicitações da ANPD, dos titulares dos dados e dos órgãos públicos os quais atue.

Tal cargo, por sua vez, poderia ser ofertado em concurso público tendo como requisito para ingresso curso superior em Direito ou curso superior ou cursando em Sistemas de Informação ou áreas afins. Pensa-se em não exigir necessariamente o curso superior completo na área de conhecimento tecnológico por conta do próprio contexto atual do Brasil: muita demanda por profissionais capacitados nas áreas de tecnologia, e poucos profissionais disponíveis no mercado. Observa-se, com o presente estudo, que a demanda por profissionais DPO, além de necessária, é latente.

Sugere-se, também, que a prova do respectivo concurso público aborde tanto

---

[22]**Lei n 12.527 de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, 18 nov. 2011a. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm >. Acesso em: 19 de dezembro de 2022. "Art. 1º, parágrafo único e incisos I e II: Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

Parágrafo único. Subordinam-se ao regime desta Lei:

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios."

conhecimentos na área do Direito, quanto conhecimentos na área de Tecnologia da Informação. Assim, os requisitos para ingresso ao cargo não impedem um número gigantesco de possíveis participantes, já que não se exige duas (02) graduações em nível superior, mas garante que os aprovados demonstrem conhecimentos necessários para o exercício da função DPO na Administração Pública.

Desta forma, espera-se que o presente estudo contribua, ao menos minimamente, para a construção de uma Administração Pública brasileira mais eficiente e coerente com a realidade atual. Através do estudo, e de sua aplicação no funcionalismo público, se constrói um país melhor para todos.

10 CONSIDERAÇÕES FINAIS

Com a análise do contexto atual do Brasil em relação ao tema da proteção de dados pessoais, fica claro que o país teve um grande avanço com a promulgação da LGPD. O surgimento da primeira lei específica no país sobre a proteção dos dados de seus cidadãos, é um marco que alcança diretamente não só os brasileiros que atuam na área do Direito, mas todos aqueles que compõem a nação, justamente por ser uma garantia daquilo que hoje é reconhecido como Direito Fundamental.

Não se pode, entretanto, achar que a elaboração da LGPD é suficiente para se ter uma plena proteção dos dados pessoais. É necessário que a LGPD seja incrementada com alterações que visem a sua melhoria, e que tenha aplicação verdadeiramente efetiva. A ANPD, o operador de dados, o controlador de dados, o profissional DPO, o legislador, os magistrados, e todos os outros que atuarem no âmbito da proteção de dados no Brasil, devem zelar para que se tenha, na prática, um ambiente de utilização correta dos dados pessoais.

A partir do presente estudo, fica claro que a Administração Pública brasileira deve se atentar para as providências a serem tomadas visando o uso regular de dados pessoais. Tanto a quantidade de dados tratados pela Administração Pública, quanto a sensibilidade de grande parte destes dados, justificam uma atenção especial dos administradores para a operação de dados no serviço público.

Neste sentido, a pesquisa aqui realizada expôs uma necessidade para a

Administração Pública brasileira, que é o trabalho dos profissionais DPO. Espera-se que tais encarregados de proteção de dados tenham espaço pleno, no Brasil, para atuar de modo compatível com as necessidades do Poder Público, e com os direitos de cada um dos cidadãos.

É com esperança que se olha para o assunto da proteção de dados pessoais no Brasil. Está claro que muito trabalho precisa ser feito, mas as normativas já começaram as mudanças de bom modo. A necessidade aqui exposta é um caminho que ainda precisa ser traçado, mas que já tem bons direcionamentos com o reconhecimento da proteção de dados pessoais como direito fundamental, e com o sistema gerado pela LGPD para a efetiva garantia da proteção dos dados pessoais no Brasil.

REFERÊNCIAS

ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil** – e suas consequências. **Jota**, São Paulo, 28 de janeiro de 2022. Disponível em: < https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022 >. Acesso em: 16 de dezembro de 2022.

BRASIL, Emanuelle e ASSUMPÇÃO, Regina Céli. Consulta pública será base para projeto de lei sobre proteção de dados pessoais. **Agência Câmara de Notícias**, 28 de janeiro de 2015. Disponível em: < https://www.camara.leg.br/noticias/449278-consulta-publica-sera-base-para-projeto-de-lei-sobre-protecao-de-dados-pessoais/ >. Acesso em: 15 de dezembro de 2022.

BRASIL. Ministério Público do Distrito Federal e Territórios**. MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados**. [Brasília]: Ministério Público do Distrito Federal e Territórios, 05 de fevereiro de 2019. Disponível em: < https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados >. Acesso em: 16 de dezembro de 2022.

BRASIL. Serviço Federal de Processamento de Dados. **Conheça os dez temas prioritários da ANPD para o biênio 2021 – 2022.** [Brasília]: Serviço Federal de Processamento de Dados (Serpro), 02 de fevereiro de 2021. Disponível em: < https://www.serpro.gov.br/lgpd/noticias/2021/anpd-agenda-regulatoria-lgpd#:~:text=A%20Autoridade%20Nacional%20de%20Proteção%20de%20Dados%20foi%20criada%20pela,5%20de%20novembro%20de%202020. >. Acesso em: 19 de dezembro de 2022.

CAMBRICOLI, Fabiana. Ministério da Saúde foi alertado em junho por ONG sobre outra exposição indevida de dados. **O Estado de São Paulo**, 27 de novembro de 2020. Disponível em: < https://www.estadao.com.br/saude/ong-alertou-ministerio-em-junho-que-dados-de-pacientes-eram-vulneraveis/ >. Acesso em: 21 de dezembro de 2022.

CAMBRICOLI, Fabiana. Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. **O Estado de São Paulo**, 02 de dezembro de 2020. Disponível em: < https://www.estadao.com.br/saude/nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes/ >. Acesso em: 21 de dezembro de 2022.

CARLOTO, Selma; BRAMANTE, Ivani Contini; CAVALINI, Juliane Pascoeto. **Lei Geral da Proteção de Dados e Segurança da Informação: Perguntas e Respostas**. 1. ed. LTr, 2022.

DONDA, Daniel. **Guia Prático de Implementação da LGPD**. 1. ed. São Paulo - SP: Labrador, 2020.

GUIMARÃES, João Alexandre; MACHADO, Lécio Silva. **Comentários à Lei Geral de Proteção de dados: lei 13.709/2018 com alterações da MPV 869/2020**. 1. ed. Rio de Janeiro - RJ: Lumen Iuris, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >. Acesso em: 19 dez. 2022.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União: Brasília, DF, 18 nov. 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm >. Acesso em: 19 dez. 2022.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018**. 2. ed. São Paulo - SP: SaraivaJur, 2020.

SÃO PAULO. Tribunal de Justiça. **Recurso Inominado Cível nº 1003086-21.2021.8.26.0003**. Recorrente: Ana Maria Nishimura da Cruz. Recorrido: Eletropaulo Metropolitana Eletricidade de São Paulo S/A. Relator: Juiz Carlos Eduardo Santos Pontes de Miranda (4ª Turma Recursal Cível). São Paulo, 25 de outubro de 2021. Disponível em: < https://jurisprudencia.s3.amazonaws.com/TJ-SP/attachments/TJ-SP_RI_10030862120218260003_921dc.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1671619144&Signature=v0emL%2BHnUs6PQzceiaJX2QHClQw%3D >. Acesso em: 21 de dezembro de 2022.