

UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

MATHEWS PINHEIRO LEITE SANTOS CORREIA

**A NOVA LEI GERAL DE PROTEÇÃO DE DADOS (13.709/18) E OS
PRINCIPAIS IMPACTOS CAUSADOS NA ATIVIDADE EMPRESARIAL**

JUAZEIRO DO NORTE-CE
2021

MATHEWS PINHEIRO LEITE SANTOS CORREIA

**A NOVA LEI GERAL DE PROTEÇÃO DE DADOS (13.709/18) E OS
PRINCIPAIS IMPACTOS CAUSADOS NA ATIVIDADE EMPRESARIAL**

Trabalho de Conclusão de Curso – *Artigo Científico*,
apresentado à Coordenação do Curso de Graduação
em Direito do Centro Universitário Doutor Leão
Sampaio, em cumprimento às exigências para a
obtenção do grau de Bacharel.

Orientador: Me. Francisco Thiago da Silva Mendes

MATHEWS PINHEIRO LEITE SANTOS CORREIA

**A NOVA LEI GERAL DE PROTEÇÃO DE DADOS (13.709/18) E OS
PRINCIPAIS IMPACTOS CAUSADOS NA ATIVIDADE EMPRESARIAL**

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de MATHEWS PINHEIRO LEITE SANTOS CORREIA.

Data da Apresentação 09 / 12 / 2021

BANCA EXAMINADORA

Orientador: Prof. Me. Francisco Thiago da Silva Mendes

Membro: Prof. Ma. Tamyres Madeira de Brito/ UNILEÃO

Membro: Prof. Me. Clauver Rennê Luciano Barreto/ UNILEÃO

JUAZEIRO DO NORTE-CE

2021

A NOVA LEI GERAL DE PROTEÇÃO DE DADOS (13.709/18) E OS PRINCIPAIS IMPACTOS CAUSADOS NA ATIVIDADE EMPRESARIAL

Mathews Pinheiro Leite Santos Correia¹
Francisco Thiago da Silva Mendes²

RESUMO

O presente trabalho discute a respeito da Lei Geral de Proteção de Dados (13.709/2018) e seus principais impactos na sociedade empresarial brasileira. Seu objetivo geral busca analisar quais são os principais impactos causados pela LGPD na atividade empresarial brasileira, seus objetivos específicos se dividem em três capítulos: O primeiro capítulo busca traçar o contexto histórico das principais leis sobre a proteção de dados que resultaram na criação da LGPD. O segundo capítulo busca descrever os principais conceitos e princípios apresentados pela legislação e por fim, o último capítulo busca apresentar os principais impactos causados pela LGPD na atividade empresarial brasileira. Trata-se de uma pesquisa do tipo básico, com objetivos exploratórios e explicativos, sua abordagem é qualitativa e sua fonte classifica-se como uma pesquisa bibliográfica e documental. Os resultados indicam que, com a entrada em vigor da LGPD e de seu órgão regulador, conhecido por ANPD (Autoridade nacional de proteção de dados), as empresas devem observar e aplicar o disposto na legislação, buscando sempre proteger os dados utilizados em suas transações, estando devidamente regulado com a ANPD, evitando assim as sanções administrativas presentes na legislação.

Palavras Chave: Lei Geral de Proteção de Dados. LGPD. Dados. Atividade empresarial.

ABSTRACT

This paper is about the General Data Protection Law (13.709/2018) and its main impacts on Brazilian business society. Its general objective seeks to analyze the main impacts caused by the LGPD on Brazilian business activity, its specific objectives are divided into three chapters: The first chapter seeks to trace the historical context of the main laws on data protection that resulted in the creation of the LGPD. The second chapter describes the main concepts and principles presented by the legislation and, finally, the last one presents the main impacts caused by the LGPD on Brazilian business activity. It is a research of the basic type, with exploratory and explanatory objectives, its approach is qualitative and its source is classified as bibliographical and documentary research. The results indicate that, with the entry into force of the LGPD and its regulatory body, known as ANPD (National Data

¹ Graduando do curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão
_pinheiromathews@gmail.com

² Professor do Centro Universitário Doutor Leão Sampaio/Unileão, Especialista em Direito Penal e Criminologia/Urc, Mestrando em Direito da Empresa e dos Negócios/UNISINOS, Advogado
_thiogomendes@leaosampaio.edu.br

Protection Authority), companies must observe and apply the provisions of legislation, always seeking to protect the data used in their transactions, being duly regulated with the ANPD, thus avoiding the administrative sanctions present in the list of legislation.

Keywords: General Data Protection Law. LGPD. Dice. Business activity.

1 INTRODUÇÃO

Ao caminhar dos anos a humanidade assistiu ao processo de revolução. Máquinas a vapor, produção em massa, revolução técnico-científico, e agora, a mesma se encontra no pináculo da era digital também conhecida como quarta revolução industrial. Neste momento, ainda que de forma indireta e silenciosa, a tecnologia se faz presente na vida de milhões de pessoas pelo mundo através da chamada inteligência artificial.

Neste cenário digital em que se encontra a humanidade, usuários dessa tecnologia correm constantemente o risco de terem os seus dados expostos ao mundo. Assim, se fez necessário pensar em medidas capazes de proporcionar a segurança de todo e qualquer dado. Desta forma, em âmbito internacional, leis foram criadas para garantir a segurança jurídica e tratamento adequado para seus dados. Nacionalmente é possível citar algumas leis que regulam o meio digital, temos, por exemplo, a Lei Nº 12.737 (BRASIL, 2021), Lei Carolina Dieckmann, Decreto Lei Nº 7.962 (BRASIL, 2013), Contratação no comércio eletrônico, Lei Nº 12.956/2014 (BRASIL, 2014), Marco civil da internet. De forma mais atual, no ano de 2018 o Brasil promulgou a Lei Nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, conhecida como LGPD. Diante de alguns modelos internacionais, a LGPD deriva do modelo Europeu de proteção de dados o *General Data Protection Regulation* (GDPR) representado hoje pelo regulamento 679/16 (PARLAMENTO EUROPEU, 2016), incorporando seus dois aspectos básicos: (I) os setores públicos e privados devem ser regulamentados por uma única lei, sendo esta de caráter geral; (II) deve existir uma autoridade fiscalizadora atuante em todo o país, no Brasil esse órgão é a Autoridade Nacional de Proteção de Dados (ANPD).

A referida lei 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.

Entre diversos aspectos legais, a lei disciplina os fundamentos da proteção de dados, o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de

informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Diante disso, a presente proposta de pesquisa destina-se a resolução do seguinte problema: Quais são os principais impactos causados pela nova lei geral de proteção de dados na atividade empresarial?

A principal razão desta pesquisa debruçar-se sobre este problema se dá não só pela extrema atualidade do tema, mas também pela sua importância, visto os riscos recorrentes do vazamento de dados. Sobre o prisma empresarial deve-se analisar quais são os principais impactos causados pela LGPD na atividade empresarial brasileira e como esta afeta esse cenário.

O presente trabalho tem como objetivo geral analisar quais são os principais impactos causados pela nova lei geral de proteção de dados na atividade empresarial brasileira.

Em se tratando dos objetivos específicos, este será dividido em três capítulos. No primeiro capítulo será traçado o contexto histórico das principais leis sobre proteção de dados que resultaram na criação da LGPD. No segundo capítulo será descrito os principais conceitos e princípios sobre a proteção de dados apresentados pela própria lei. Por fim, o último capítulo busca analisar e apresentar os principais impactos e alterações causadas pela nova lei geral de proteção de dados na atividade empresarial brasileira.

Diante da complexidade do tema, de sua extrema atualidade e importância para a sociedade empresarial, requer um estudo aprofundado acerca da lei e sua aplicação às empresas de grande ou pequeno porte. Assim este trabalho é de suma importância a todos os empresários que necessitam de adequação às normas da LGPD evitando a aplicação de sanções administrativas por parte do órgão regulador (ANPD). Além disso, o presente trabalho terá contribuição para comunidade acadêmica, ao passo em quem se enquadra como suporte ou até mesmo como fonte para outros pesquisadores.

A presente proposta de pesquisa classifica-se na área de ciências sociais aplicadas, dentre as quais encontra-se o Direito. Quanto a sua natureza, esta se classifica em uma pesquisa básica, a qual, segundo Denise Tolfo Silveira e Fernanda Peixoto (2009) este tipo de pesquisa busca gerar novos conhecimentos essenciais ao avanço científico. Quanto a seus objetivos, esta pesquisa é exploratória, segundo Gil (2007) a pesquisa exploratória busca possibilitar maior contato com o problema, e a pesquisa explicativa, segundo o referido autor,

este tipo de pesquisa preocupa-se em determinar fatos que contribuem na ocorrência de fenômenos e na explicação do por que destes.

Quanto à abordagem, tem-se a pesquisa qualitativa, a qual, segundo Deslauriers (1991) deve produzir informações, não importando o tamanho destas, apenas as informações obtidas. Quanto às fontes, esta pesquisa é bibliográfica e documental. Segundo Fonseca (2002) a pesquisa bibliográfica é o início de qualquer trabalho, pois é feita a partir do levantamento de referências teóricas que já foram analisadas, estas podem ser por livros, artigos científicos ou páginas de web site. Ainda para Fonseca, a pesquisa documental segue o mesmo percurso da pesquisa bibliográfica recorrendo a outros meios como documentos oficiais, atas, cartas, filmes, revistas e etc.

Assim, a presente pesquisa busca gerar conhecimento científico através do contato com o problema e da futura explicação deste através de levantamento bibliográfico e documental de livros, artigos científicos e da própria legislação acerca do tema.

2 CONTEXTO HISTÓRICO DAS PRINCIPAIS LEIS SOBRE A PROTEÇÃO DE DADOS QUE RESULTARAM NA CRIAÇÃO DA LEI 13.709/18 – LGPD

As questões acerca da proteção de dados têm sido palco de inúmeros debates nos últimos tempos. A lei nº 13.709/18 acentuou os debates sobre o tema tornando-se mais evidenciado pelo fato de seu órgão regulador ter iniciado sua função coercitiva em agosto de 2021. Embora muito atual, as discussões acerca da proteção de dados decorrem de uma longa linhagem temporal.

O contexto histórico da proteção de dados tem início com a concepção do direito à privacidade. Segundo Mendes (2014) a discussão acerca da privacidade se inicia em 1890, quando os advogados americanos Samuel D. Warren e Louis Brandeis publicaram um artigo jurídico intitulado de “*The right to privacy*” (O Direito a Privacidade), que, até hoje é considerada como a primeira publicação sobre o assunto e uma das mais influentes no território estadunidense.

Segundo Zanon (2013), antes do referido artigo, já era possível enxergar o início da caminhada para o que se entende hoje como direito a privacidade, quando o jurista norte-americano Thomas McIntyre Cooley (1824-1898) em 1888 publicou sua obra intitulada “*A Treatise on the Law of Torts*” (Um tratado sobre a lei de delitos) onde utilizou a expressão “*Right to be let alone*” (o direito de estar só). Ocorre, entretanto que a publicação não era ligada a noção de privacidade e sim sobre a responsabilidade civil. Porém, mesmo em se

tratando de outro tema, a expressão utilizada pelo autor teve grande influência em trabalho publicado pelos advogados anos depois sobre o direito à privacidade.

Para Zanini, ao dissertar sobre o contexto histórico do Direito a Privacidade:

A expressão forjada por Cooley somente ganhou relevo com a publicação, em 15 de dezembro de 1890, na *Harvard Law Review*, do artigo de autoria de Samuel D. Warren e Louis D. Brandeis, intitulado *The right to privacy*. Nele, os autores colocam em evidência a ocorrência de transformações sociais, políticas e econômicas, bem como o surgimento de novos inventos, como a fotografia, que contribuíram para a ocorrência de violações da vida privada das pessoas. (ZANINI, 2015, p. 05)

Assim, oficialmente, foi no ano de 1890, com a publicação do artigo “*The right to privacy*” na revista *Harvard Law Review* que se inicia o contexto de privacidade que vem a se tornar direito tutelado pela LGPD (ZANINI, 2015).

Mais tarde, no ano de 1948 a ONU (Organização das Nações Unidas) promulgou a Declaração Universal dos Direitos Humanos em resposta aos terríveis acontecimentos ocorridos na primeira e segunda guerra mundial. Dentre outros direitos, a Declaração dispõe em seu artigo 12 que “ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (ONU, 1948).

No ano de 1970, com o avanço da tecnologia computacional surgem as primeiras leis gerais de proteção de dados no Estado de Hesse na Alemanha intitulada de *Hessische Datenschutzgesetz* (Lei de proteção de dados de Hesse), a qual regula quando a administração pública do Estado de Hesse pode tratar sobre dados pessoais buscando proteger os usuários e a estrutura constitucional do Estado de ser ameaçada pelo processamento automatizado de dados.

Segundo Mendes (2004) é aproximadamente neste período de 1970 que se iniciam as decisões legislativas afirmando que os dados pessoais são projeções do indivíduo, assim, passíveis da tutela jurídica.

Seguindo a linha do tempo, em 1993 o Governo Sueco aprovou o “*Data Protection Act*” e o “*Privacy Act*”, o que serviu de modelo para outros países europeus.

A preocupação com a proteção e confidencialidade das informações pessoais constantes de bancos de dados remonta à metade do século XX, sendo que alguns países, desde a década de 1970, já haviam aprovado leis para tratar do assunto, como, por exemplo, o “*Data Protection Act*” (que, em suma, proibia a abertura de registros de dados sem permissão oficial e estabelecia um conselho para proteção de dados pessoais, para supervisão de tais atividades), aprovado pelo governo sueco, em 1973, e o “*Privacy Act*” (que, em síntese, proibia a divulgação de informações pessoais por agências governamentais sem o prévio consentimento da pessoa envolvida) aprovado pelo governo norte-americano, em 1974. Em 1978, normas semelhantes foram adotadas por outros países europeus, como Alemanha e França. (TAVARES E ALVAREZ, 2018)

Segundo Krieger (2019) mesmo havendo documentos anteriores a respeito da proteção de dados, somente em 1980 que os países europeus passam a ter uma maior preocupação com o tema. Em 1981 ocorreu na Europa a Convenção de Strasbourg Nº 108 do Conselho Europeu que tratou o direito à vida privada como um direito fundamental logo em seu artigo 1º³.

Conforme o artigo supracitado todas as pessoas, independente de sua nacionalidade possuem a tutela jurídica a seus direitos fundamentais e demonstra ênfase ao se referir à vida privada diante do tratamento de dados.

No ano de 1995 a União Europeia promulga a Diretiva 95/46/CE que estabelece as diretrizes pertinentes a cada Estado-Membro da União Europeia para que cada um deste adotasse sua própria legislação relativa a proteção de dados. Neste sentido, o site EUR-Lex.europa.eu, o qual dá acesso à legislação da União Europeia dispõe:

A Diretiva 95/46/CE constitui o texto de referência, a nível europeu, em matéria de proteção dos dados pessoais. Institui um quadro regulamentar a fim de estabelecer um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais no interior da União Europeia (UE). Para este efeito, fixa limites estritos à recolha e à utilização de dados pessoais e solicita a criação, em cada Estado-Membro, de um organismo nacional independente encarregado do controlo de todas as atividades relacionadas com o tratamento de dados pessoais. (União Europeia, 1995)

Segundo Lopes, (Anuário de proteção de dados, 2018), a Diretiva foi revogada anos depois em 2016 pelo regulamento 679/46 conhecido como GDPR “*General Data Protection Regulation*” (Regulamento geral de proteção de dados - RGPD). Neste momento, se entende a proteção de dados de pessoas singulares, ao tratamento de seus dados pessoais e sobre a livre circulação destes dados, tendo como objetivo a modernização e a harmonização das regras de proteção de dados entre os Estados-Membros.

Segundo Krieger (2019), em solo nacional, a proteção de dados tem início com a promulgação da Constituição Federal de 1988, a qual prevê como forma de proteger os direitos fundamentais, prevendo resguardar o direito a intimidade e à vida privada, previsto no art. 5º, inc. X. Além disso, foi mantida a inviolabilidade do domicílio, previsto no art. 5º, inc. XI e o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, previsto no art. 5º, inc. XII.

Doneda (2006, p. 142) entende que a privacidade assume um novo patamar ao que tange a proteção da pessoa humana, não sendo esta apenas um “escudo contra o exterior”, mas

³ Artigo 1.º Objetivos e finalidade: A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («proteção dos dados»). (Conselho Europeu. 1981)

também como um elemento indutor da cidadania, “da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral”.

Segundo a plataforma de monitoramento, resgate e análise sobre a privacidade e proteção de dados no Brasil, Observatório da privacidade, a iniciativa brasileira para a criação de uma lei específica para a proteção de dados se dá no ano de 2010 quando o Ministério da Justiça iniciou consultas públicas com a finalidade de delimitar o anteprojeto de Lei de Proteção de Dados ligados ao Ministério de Desenvolvimento, Indústria e Comércio Exterior (MDIC). No entanto, é somente no ano de 2015 através do Projeto de Lei 5276/16 que o assunto volta a ser discutido.

Em 2011 há um importante marco com a promulgação da Lei 12.527, a lei de acesso à informação. A qual institui como princípio fundamental que o acesso à informação pública é a regra, e o sigilo somente a exceção. Para garantir o exercício pleno do direito de acesso previsto na Constituição Federal, a referida lei 12.527/11 define os mecanismos, prazos e procedimentos para a entrega das informações solicitadas à administração pública pelos cidadãos. A Lei igualmente determina que os órgãos e entidades públicas deverão divulgar um rol mínimo de informações proativamente por meio da internet. (BRASIL, 2011.)

Em 2012, o Projeto Lei nº 2.793/2011 se tornou a Lei 12.737, conhecida como Lei Carolina Dieckmann. O famoso caso ocorreu quando a atriz brasileira, a qual dá o nome à lei, teve o seu computador pessoal invadido e a sua vida privada exposta em um ato de ataque virtual. A lei acrescentou ao Código Penal Brasileiro os artigos 154-A e 154-B além de alterar a redação dos artigos 266 e 298 do mesmo dispositivo legal.

O célere crescimento tecnológico e a rápida propagação de informações demonstram uma nova preocupação. Dessa vez no cenário digital, assim no ano de 2014 surgem novas regras para o uso de internet no Brasil com a Lei 12.965, o marco civil da internet. A lei trouxe garantias acerca da privacidade e da proteção de dados pessoais, além disso, estabeleceu regras, princípios, direitos e deveres para usuários de internet brasileira.

Sobre o referido assunto, o professor Schreiber (2015) leciona que a internet é usualmente vista como uma aliada da liberdade de expressão. Sua capacidade de “amplificar” o alcance das manifestações individuais é frequentemente apontada como um estímulo à livre circulação das ideias.

Finalmente, em 14 de agosto de 2018, após inúmeros adiamentos foi promulgada a Lei Geral de Proteção de Dados (LGPD) a qual deveria entrar em vigor após 18 meses, em fevereiro de 2020. Em novembro do mesmo ano foi promulgada a M.P 869/18 a qual visa á

criação da Autoridade Nacional de Proteção de Dados (ANPD) e muda a entrada em vigor da LGPD para 24 meses (agosto de 2020).

No ano de 2019 foi promulgado o Decreto 9936/19 que disciplina a formação e consulta em bancos de dados com informações de adimplemento para a formação do histórico de crédito no Brasil (*score*).

Após isso, entre outubro de 2019 e março de 2020 foram propostos alguns Projetos de Lei para adiar a entrada em vigor da LGPD, até mesmo em virtude da pandemia causada pelo SARS-CoV-2 (Covid-19). No entanto, estes não foram acatados e em junho de 2020, depois de uma longa evolução histórica foi sancionado o Projeto de Lei 1179/20, o qual mantém a vigência da LGPD para 1º de agosto do mesmo ano. A LGPD É um marco legal que regulamenta o uso, a proteção e a transferência de dados pessoais no Brasil, a Lei 13.709/2018 garante maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados. (BRASIL, 2018).

Por fim, no dia 6 de novembro de 2020, iniciou a operar à Agência Nacional de Proteção de dados (ANPD), conforme estava disciplinado nos artigos 52, 53 e 54 da LGPD. A ANPD trata-se de um órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento adequado da LGPD em território nacional. E através desse órgão que as sanções administrativas serão aplicadas aqueles que descumprirem as normas estabelecidas pela legislação (BRASIL, 2021).

3 PRINCIPAIS CONCEITOS E PRINCÍPIOS SOBRE A PROTEÇÃO DE DADOS APRESENTADOS PELA LEGISLAÇÃO

De fato, a LGPD trouxe inúmeros conceitos e princípios a serem observados pelo operador de dados. Então, para que de fato os dados sejam devidamente tratados, deve-se entender, a priori, os principais objetivos da lei. Segundo a plataforma LGPD Brasil, a Lei Geral de Proteção de Dados possui seis objetivos, os quais torna ainda mais visível à importância da lei.

O primeiro objetivo é a proteção de dados, segundo a Plataforma LGPD Brasil, a lei busca assegurar o direito à privacidade e a proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais. O segundo objetivo é a transparência que busca estabelecer regras claras sobre tratamento de dados pessoais. O

terceiro objetivo é o desenvolvimento que visa fomentar o desenvolvimento econômico e tecnológico.

O quarto objetivo é a padronização de normas, que busca estabelecer regras únicas e harmônicas sobre tratamento de dados pessoais, por todos os agentes e controladores que fazem tratamento e coleta de dados. O quinto objetivo é a própria segurança jurídica que visa o fortalecimento da segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo. Por fim, o sexto objetivo é o favorecimento à concorrência, visando promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

Mencionado os principais objetivos da lei, a própria legislação, em seu artigo 5º apresenta um rol conceitual de importante conhecimento, afinal, são os conceitos e princípios que norteiam a aplicabilidade da legislação por parte do operador.

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

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

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

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X - 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;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - 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;

XVII - relatório de impacto à proteção de dados pessoais: 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;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

(BRASIL, 2018)

A própria legislação é autoexplicativa, o artigo 5º preocupou-se em apresentar a todos os agentes envolvidos no tratamento de dados os devidos conceitos a que se tratam, não somente os dados, mas também os agentes e órgãos.

Uma importante definição extraída pela lei é sobre os dados e os diferentes tipos de dados. O primeiro diz respeito aos dados pessoais, segundo a Plataforma LGPD Brasil, os dados pessoais previstos no artigo 5º, inciso I da Lei diz respeito a tudo aquilo que pode identificar uma pessoa, números, características pessoais, qualificação pessoal, dados genéticos e etc.

Os dados sensíveis, previstos no inciso II do artigo 5º da Lei, são aqueles dados ou informações que podem ser utilizados de forma discriminatória, assim sendo, carecem de proteção especial. (LGPD Brasil, 2021)

Já os dados anonimizados⁴ é o dado relativo a titular que não possa ser identificado, considerado a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, em outras palavras é um dado pessoal ou um dado sensível que foi tratado afim de que as informações relativas a ele não sejam vinculadas ao seu titular. Está previsto no artigo 5º, inciso III da Lei. Devido a sua anonimização, estes estariam fora do escopo de aplicação da lei, à exceção se o processo de anonimização puder ser revertido ou se estes forem utilizados na formação de perfis comportamentais.

Dados efetivamente anonimizados são essenciais para o funcionamento de tecnologias no campo da Internet das Coisas, inteligência artificial, *machine learning*, *smart cities* e análise de grandes contextos comportamentais. (LGPD Brasil, 2018)

Outro dado que necessita de atenção são os dados pessoais de crianças e adolescentes, previstos no artigo 14 da LGPD⁵, para estes foram criados uma seção específica, visto que se tratando de crianças e adolescentes, os dados devem ser realizados em seu melhor interesse. (BRASIL, 2021)

Os conceitos e princípios são de suma importância para aplicação da lei. Segundo o Jurista Celso Antônio Bandeira de Mello (2009), os princípios constituem um verdadeiro alicerce a quem precisa de sua compreensão. Assim, a LGPD apresenta em seu artigo 6º um rol de princípios, dentre os quais, o famoso Princípio da Boa-fé.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - 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;

IV - 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;

V - 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;

⁴ Dados anonimizados diz respeito aos dados pessoais ou sensíveis que, originariamente, era relativo a uma pessoa, mas que passou por tratamentos para ser desvinculado dessa pessoa.

⁵ Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente (Brasil, 2021).

VI - 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;

VII - 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - 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.

(BRASIL, 2018)

Da mesma forma como os conceitos foram postos na legislação, os princípios também são autoexplicativos.

Juntamente do Princípio da Boa-fé, o primeiro princípio apresentado pela lei é o Princípio da Finalidade, previsto no artigo 6º, inciso I, o qual se traduz na ideia de que o dado deverá, na coleta, ter a indicação clara e completa que a justifique. Assim, realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (BRASIL, 2021)

O inciso II do mesmo artigo apresenta o Princípio da Adequação, o qual se perfaz na ideia de que os dados devem ser tratados de acordo com a sua destinação. A coleta de dados deverá ser compatível com a atividade fim do tratamento. (BRASIL, 2021)

O princípio previsto no artigo 6º, inciso III trata-se do Princípio da Necessidade o qual descreve que a coleta de dados deve ocorrer de forma restritiva, cuidando para que o tratamento dos dados pessoais esteja restrito à finalidade pretendida. O tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (BRASIL, 2021)

Em seguida, o inciso IV do artigo 6º traz como princípio norteador o livre acesso, o qual possibilita que o titular dos dados consulte livremente, de forma facilitada e gratuita, a forma e a duração do tratamento dos dados, bem como sobre a integralidade deles. (BRASIL, 2021)

No artigo 6º, inciso V apresenta a qualidade dos dados. Este princípio busca garantir aos titulares dos dados a exatidão, a clareza, a relevância e a atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. (BRASIL, 2021)

O inciso VI apresenta o Princípio da Transparência, o qual visa garantir aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento dos dados. (BRASIL, 2021)

Em seguida, o inciso VII do mesmo artigo, apresenta ao operador o Princípio da Segurança. Este compreende medidas técnicas e administrativas para proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. (BRASIL, 2021)

O inciso VIII, norteia o Princípio da Prevenção, o qual é um dos pilares da Segurança da Informação, buscando a antecipação de eventualidades, com a adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais. (BRASIL, 2021)

O Princípio da Não Discriminação, previsto no artigo 6º, inciso IX, este diz que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos, ou seja, não se pode excluir de titulares de dados pessoais, no momento de seu tratamento, informações determinadas por características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual. (BRASIL, 2021)

Por fim, o último princípio, previsto no artigo 6º, inciso X é o Princípio da Responsabilização e Prestação de Contas o qual, espera-se que o controlador ou o operador demonstrem todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas. (BRASIL, 2021)

4 ANALISE DOS PRINCIPAIS IMPACTOS E ALTERAÇÕES CAUSADOS PELA NOVA LEI GERAL DE PROTEÇÃO DE DADOS NA ATIVIDADE EMPRESARIAL BRASILEIRA

A LGPD busca a proteção de dados diante do fato de que um dado solto e desconexo pode parecer inofensivo, mas a junção de vários dados torna-se um perigo. Esta é a ideia principal da teoria do mosaico apresentada por Conesa.

Existem dados a priori irrelevantes do ponto de vista do direito à privacidade e que, no entanto, em relação a outros, talvez também irrelevantes, podem servir para tornar a personalidade de um cidadão totalmente transparente, tal como acontece com as pedrinhas. Que em si mesmos nada dizem, mas que juntos podem formar conjuntos completos de significados. (CONESA, 1984, traduzido)

Assim, cabe ao Controlador, ao Operador e ao Encarregado a proteção de dados do Titular. Dentro da atividade empresarial não é diferente, visto que a LGPD se aplica a todo o cenário nacional. Com a entrada em vigor da LGPD em 2018 as empresas, de grande ou de pequeno porte tiveram que se adequar as normas da legislação vigente ao passo que essa é detentora de informações pessoais de seus empregados, colaboradores e até de seus clientes.

Temos, no caput do artigo 966 do Código Civil que “Considera-se empresário quem exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços.” (BRASIL, 2002).

Assim, com base no artigo supracitado, o doutrinador André Luiz Santa Cruz Ramos apresenta uma clara definição sobre a empresa e o empresário, sendo a empresa uma atividade econômica organizada com a finalidade de fazer circular ou produzir bens ou serviços, por sua vez, o empresário é quem exerce empresa.

A plataforma virtual LGPD Brasil, prevê que a Lei Geral de Proteção de dados terá grande impacto nas relações comerciais e de consumo que demandam coleta de dados

Fica claro então, que o primeiro impacto da LGPD nas empresas é a própria adequação destas a legislação vigente. Diante do constante risco para atividade empresarial, a plataforma LGPD Brasil listou doze formas/etapas que as empresas devem fazer para alcançar a adequação frente à LGPD.

A primeira diz respeito à *Due Diligence* sobre dados pessoais, segunda a mesma plataforma, deve-se identificar os dados (pessoal, sensível, criança, público, anonimizado), departamentos, meios (físico ou digital), operadores internos e externos para mensuração de exposição da empresa à LGPD. (LGPD BRASIL, 2021)

Para Camargos e Barbosa, 2009, este tipo de procedimento tem por finalidade uma análise minuciosa das variáveis e condições envolvidas na negociação.

A tradução literal de “*Due Diligence*”⁶ é devida cautela, ponto em que muitos autores afirmam que seu papel é uma revisão aprofundada em informações.

Sobre o assunto, leciona Fachinetti e Poggio que ponto de partida para a análise são documentos como, políticas de privacidade, políticas de gestão de incidentes, relatórios da auditoria interna ou externa e afins.

⁶ Ribeiro (2001) define a *due diligence* como um procedimento que identifica os aspectos econômicos, financeiros, e físicos, entre os quais fazem parte as variáveis ambientais que estejam afetando, ou poderão vir a afetar, a situação patrimonial de uma companhia.

A segunda etapa é a Auditoria, a qual trata da à Aderência das 20 atividades de tratamento de dados e aos princípios gerais da LGPD, mediante revisão e criação de documentos (contratos, termos, políticas) para uso interno e externo (LGPD BRASIL, 2021).

Em sua obra “Auditoria”, Boynton, Johnson e Kell (2002) utilizam a definição criada pelo *Report of the Committee on Basic Auditing Concepts of the American Accounting Association* para descrever a auditoria como um processo sistemático de obtenção e avaliação objetivas de evidências sobre afirmações a respeito de ações e eventos econômicos de comunicação dos resultados a usuários interessados.

Ainda segundo a plataforma, a próxima etapa é a Gestão dos pedidos do titular, o qual trata sobre o controle do consentimento e anonimização para atender possível solicitação do titular e da futura agência.

O artigo 5º, inciso XII da Lei nº 13.709/18 define consentimento como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (BRASIL, 2018)

Para fins da LGPD, o consentimento é um dos pilares da lei, o caput do artigo 7º e o inciso I deixam evidente que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular. (BRASIL, 2018).

Tepedino e Spadaccini pontuam que a base legal do consentimento para o tratamento de dados do titular representa instrumento de autodeterminação e livre construção da esfera privada, permitindo escolhas que refletem diretamente na personalidade do indivíduo.

Mais à frente o art. 8º da LGPD define que o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, se escrito, deverá constar de cláusula destacada das demais cláusulas contratuais. Este pode ser revogado a qualquer tempo mediante manifestação do titular por procedimento facilitado (BRASIL, 2018).

O instituto da anonimização está definido no artigo 5º, inciso III da LGPD, ao se tratar de dado anonimizado, sendo este um dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

A LGPD ainda trata a anonimização de dados como um dos requisitos para o tratamento de dados pessoais, e ainda entende que o processo de anonimização de dados é um direito do titular (BRASIL, 2021)

Para Martins e Faleiros Júnior, 2019, p.61, a anonimização trata-se do processo técnico que nada mais representa do que a dissociação entre determinado dado pessoal e o seu respectivo titular.

A lei também fala sobre a dispensa da exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na LGPD. (BRASIL, 2018). Mas, ressalva que, a eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas na Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. (BRASIL, 2018)

Seguindo a plataforma LGPD Brasil, a próxima etapa é a gestão dos pedidos do titular, que se perfaz na ideia de criação de banco de dados para controle dos pedidos dos titulares dos dados (acesso, confirmação, anonimização, consentimento, portabilidade etc.)

Christopher J. Date, em sua obra Introdução a Sistemas de Bancos de Dados, apresenta a seguinte definição:

Um sistema de banco de dados é basicamente um sistema computadorizado de manutenção de registros; em outras palavras, é um sistema computadorizado cuja finalidade geral é armazenar informações e permitir que os usuários busquem e atualizem essas informações quando as solicitar. As informações em questão podem ser qualquer coisa que tenha algum significado ao indivíduo ou à organização a que o sistema deve servir – ou seja, qualquer coisa que seja necessária para auxiliar no processo geral das atividades desse indivíduo ou dessa organização. (DATE, 2004, P. 6)

Assim, o banco de dados é, em resumo, um sistema que armazena informações. Com a vigência da ANPD, órgão fiscalizador e pleno para aplicação de sanções administrativas, com previsão na própria LGPD, os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, ficam sujeitos a essas sanções, entre elas a suspensão parcial do funcionamento do banco de dados a que se refere à infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador. (BRASIL, 2018)

A quinta etapa, atendendo a ANPD e demais órgãos do Sistema Nacional de Proteção do Consumidor que poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais (LGPD BRASIL, 2021)

O artigo 38⁷, a LGPD dispõe que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. (BRASIL, 2018)

O relatório de impacto é de responsabilidade do controlador e não do encarregado pelo tratamento de dados pessoais. Este, sendo o profissional que conhece a fundo a LGPD, deverá analisar o relatório e dar um parecer, mas a elaboração é do controlador. (LGPD BRASIL 2021)

Para Cecilia, o relatório de impacto (RIPD) não deve ser vista apenas como uma documentação gerada pelo controlador após um processo de conformidade. Deve ser visto como um instrumento de apoio nas atividades de tratamento de uma organização de modo que ela demonstre conformidade com as obrigações legais.

Ainda segundo a LGPD Brasil, é preciso adoção das medidas de segurança da informação aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

Fontes (2006) define a segurança da informação como as orientações, normas, procedimentos, políticas e demais ações que visam proteger a informação, possibilitando que a organização realize seu negócio e alcance sua missão.

Adiante, é preciso que as empresas se atentem a criação de regras de boas práticas e de governança que estabeleçam procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais. (LGPD BRASIL, 2021)

A lei 13.709/18 dispõe que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (BRASIL, 2018)

A legislação é clara ao dispor que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os

⁷ Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (BRASIL, 2018)

Ao seguir a linha de raciocínio da plataforma online LGPD Brasil, a próxima etapa que se verifica é adoção Plano de Comunicação – incidente de segurança.

Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais. (ANPD, 2021)

Cabendo ao controlador notificar aos órgãos fiscalizatórios (Agencia Nacional de Proteção de Dados – ANPD; Programa de Proteção e Defesa do Consumidor – PROCON; Secretaria Nacional do Consumidor – SENACON) e à imprensa sobre incidente de segurança que acarrete risco ou dano. (LGPD BRASIL, 2021)

Após a comunicação, 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. (BRASIL, 2018)

A próxima etapa é a validação do término do tratamento através da adoção das providências necessárias à eliminação dos dados tratados e verificação de eventual conservação dos dados com a elaboração de documentos que evidenciem a eliminação. (LGPD BRASIL, 2021)

Segundo a LGPD, em seu artigo 15 o término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: (I) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (II) fim do período de tratamento; (III) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou (IV) determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018)

Assim, na incidência das hipóteses acima, a lei determina que os dados pessoais sejam eliminados. A LGPD trata a exclusão como a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado. (BRASIL, 2018).

Ademais, a eliminação de dados é tratada pela LGPD no artigo 18, IV como um direito do titular. (BRASIL, 2018). No fim, o responsável deverá informar, de maneira imediata, aos

agentes de tratamento com os quais tenha realizado a eliminação, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (BRASIL, 2018)

A próxima etapa a ser tomada pelas empresas é a certificação por auditoria especializada das práticas relacionadas à LGPD. (LGPD BRASIL, 2021)

A penúltima etapa trata sobre *Data Protection Officer* - DPO (encarregado). Segundo a plataforma virtual LGPD Brasil, diz respeito à identificação do encarregado (Pessoa Física ou Jurídica) e sua capacitação para exercer as atividades previstas na LGPD.

A legislação trata o encarregado como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. (BRASIL, 2018)

Em seu artigo Panorama Geral Da Lei Geral De Proteção De Dados Pessoais No Brasil e a Inspiração no Regulamento Geral De Proteção de Dados Pessoais Europeu, a professora Regina Linden Ruaro, definiu bem o papel do DPO:

A legislação brasileira foi muito mais genérica que a europeia, inclusive nesta, há menção expressa que o DPO é uma obrigação específica para empresas com mais de 250 funcionários. Tal limitação pode vir a ser indicada pela Autoridade Nacional de Proteção de Dados no Brasil, porém até o momento toda e qualquer empresa que trate dados pessoais de forma online ou offline deverá ter um DPO, assim como cumprir todas as normas previstas na lei 13.709.(RUARO, 2019, p.352)

As atividades do encarregado consistem em: (I) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; (II) receber comunicações da autoridade nacional e adotar providências; (III) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (IV) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, 2018)

A décima segunda etapa listada pela plataforma online LGPD Brasil é a prevenção de conflitos através da Inclusão de uma cláusula compromissória de mediação vinculada à câmara privada online cadastrada no CNJ para mitigação do contencioso judicial.

Outro impacto direto da LGPD na atividade empresarial diz respeito aos requisitos para o tratamento de dados pessoais. Como visto em momento anterior, um dos principais pontos da LGPD é o consentimento do titular de dados. Assim, as empresas devem, não somente obter o consentimento, escrito ou por outro meio que demonstre a manifestação do titular (BRASIL, 2018), mas seguir todo o rol previsto no artigo 7º da Lei 13.709/18 que trata das hipóteses legais para o tratamento de dados.

Segundo a lei, o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. (BRASIL, 2018)

Importante salientar que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso. (BRASIL, 2018)

Logo, ao titular deve ser disponibilizado: (I) finalidade específica do tratamento; (II) forma e duração do tratamento, observados os segredos comercial e industrial; (III) identificação do controlador; (IV) informações de contato do controlador; (V) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (VI) responsabilidades dos agentes que realizarão o tratamento; e (VII) direitos do titular, com menção explícita aos direitos contidos no art. 18 da lei. (BRASIL, 2018)

No processo de tratamento de dados, pode o titular, obter do controlador, em relação aos dados por ele tratados, a qualquer tempo e mediante requisição a confirmação da existência de tratamento, o acesso aos dados, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei, a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial, a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD⁸, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, e a revogação do consentimento, nos termos do § 5º do art. 8º da LGPD⁹. (BRASIL, 2018)

⁸ Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

⁹ § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Assim como há hipóteses para o tratamento de dados, a lei também prevê as hipóteses de isenção da responsabilidade pelo tratamento de dados. Segundo o artigo 43 da lei 13.709/18 os agentes de tratamento só não serão responsabilizados quando provarem: (I) que não realizaram o tratamento de dados pessoais que lhes é atribuído; (II) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou (III) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018)

O Guia de Elaboração de Termo de Uso e Política de Privacidade para Serviços públicos criados pelo Governo Federal explica que os serviços públicos que demandem a utilização obrigatória dos dados pessoais do usuário, por força da legislação vigente, estão dispensados da necessidade de consentimento para tratamento dos dados, observados em qualquer caso os artigos 23 a 32 da Lei nº 13.709, de 14 de agosto de 2018. Nessa hipótese, o usuário deverá ser cientificado sobre tal uso obrigatório em decorrência de lei ou outro ato normativo. (BRASIL, 2021)

Um impacto, direto e importante que a LGPD apresentou, e que a sociedade empresária deve, não somente conhecer, mas também respeitar, diz respeito aos direitos dos titulares de dados.

A LGPD dispõe que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da LGPD. (BRASIL, 2018)

A LGPD dispõe que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (I) confirmação da existência de tratamento; (II) acesso aos dados; (III) correção de dados incompletos, inexatos ou desatualizados; (IV) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; (V) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (VI) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei; (VII) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (VIII) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; (IX) revogação do consentimento, nos termos do § 5º do art. 8º da Lei. (BRASIL, 2018)

O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional, opondo-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto da lei. Estes direitos serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. (BRASIL, 2018)

Um fato de suma importância e que afeta diretamente as empresas trazendo grande impacto sobre estas, são as sanções administrativas aplicadas aos agentes de tratamento de dados em razão das infrações cometidas às normas previstas na legislação. Esta não é necessariamente um impacto, mas, uma consequência direta do descumprimento aos impactos anteriores.

Estas sanções são competências da Autoridade Nacional de Proteção de Dados – ANPD. Este é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil.

A própria LGPD define as competências da ANPD em seu artigo 55, alínea J, dentre eles, zelar pela proteção dos dados pessoais, nos termos da legislação; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação (BRASIL, 2018)

Sobre as sanções administrativas, estas estão previstas no artigo 52 da LGPD, e variam de advertência, com indicação de prazo para adoção de medidas corretivas a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros legais. Nos termos da lei, a aplicação dessas sanções não substitui a aplicação de sanções administrativas, civis ou penais definidas no Código de Defesa do Consumidor e em legislação específica.

5 CONSIDERAÇÕES FINAIS

Ao término do presente trabalho, onde se buscou conhecer o contexto histórico das principais leis que resultaram na criação da LGPD, os principais conceitos e princípios e, por fim, os principais impactos causados pela LGPD na atividade empresarial brasileira, pode-se constatar que, após uma longa caminhada histórica, com início em 1890, tratando-se inicialmente do direito à privacidade, hoje, a proteção de dados figura como questão de suma

importância na sociedade empresarial, consumerista, e em todas as esferas onde há tratamento de dados, inclusive nos meios digitais.

Até o presente momento, ora pela atualidade, ora pela necessidade de conhecimento aprofundado do comportamento das empresas diante da LGPD, e da fiscalização por parte da ANPD o estudo identificou cinco impactos diretos da LGPD na atividade empresarial brasileira: (I) adequação as normas da Lei nº 13.709/18; (II) requisitos para o tratamento de dados; (III) dispensa do consentimento e a “não desobrigação” de cumprimentos de obrigações legais; (IV) direitos dos titulares de dados, e (V) sanções administrativas.

Ao decorrer do trabalho, lacunas foram encontradas, entendendo que, nesse momento, muito se preocupou em conhecer a LGPD, as pessoas a qual a legislação protege e aos consumidores, mas, ao adentrar na esfera empresarial percebe-se que, as questões acerca dessa área ainda são abstratas e pouco exploradas, e até mesmo embarcadas dentro de outros ramos, como o Direito Civil.

Diante disso, em estudos posteriores, sugere-se analisar a atuação das empresas no primeiro ano de vigência da Agência Nacional de proteção de dados – ANPD. Ouve uma correta adequação das empresas as normas da LGPD? Como se deu a fiscalização por parte desse órgão? Como se da atuação do DPO nas empresas após a promulgação da LGPD e da ANPD? LGPD como direito e garantia fundamental (PEC. 17).

A lei 13.709/18 foi de suma importância para realização deste trabalho, visto que a mesma é bastante autoexplicativa, e na falta do que busquei escrever, de forma mais específica, foi à própria legislação que norteou a escrita deste.

REFERÊNCIAS

2010 - 2015: **O tema entra em pauta - Observatório - Por Data Privacy, Observatório - Por Data Privacy**, disponível em:
<<https://www.observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/>>, acesso em: 3 Jun. 2021.

ANPD, Autoridade Nacional de Proteção de Dados, disponível em:
<<https://www.gov.br/anpd/pt-br>>, acesso em: 28 Aug. 2021.

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

CAMARGOS, Marcos Antônio de; BARBOSA, Francisco Vidal. Fusões e aquisições de empresas brasileiras: criação de valor e sinergias operacionais. Revista de Administração de Empresas, v. 49, n. 2, p. 206-220, abr./jun. 2009

CEDIS | **Anuário da Proteção de Dados – 2018**, Fd.unl.pt, disponível em: <<https://cedis.fd.unl.pt/blog/project/anuario-da-protecao-de-dados-2018/>>, acesso em: 3 Jun. 2021.

CONESA, F. Derecho a la intimidad, informática y Estado de Derecho. Valencia: Universidad, 1984, pp. 44-45

Constituição Federal/88. Planalto.gov.br. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 21 Maio 2021.

Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal | Portal do Ministério Público - Portugal. Ministeriopublico.pt. Disponível em: <<https://www.ministeriopublico.pt/instrumento/convencao-para-proteccao-das-pessoas-relativamente-ao-tratamento-automatizado-de-dados-2>>. Acesso em: 21 Maio 2021.

CRUZ, André Santa, **Direito Empresarial** volume único. Editora Método. 2020

Da privacidade à proteção de dados pessoais. 1. ed. Rio de Janeiro: Renovar, 2006.

DA REDAÇÃO JOTA, **Proteção de dados, due diligence e novos negócios | JOTA, JOTA Info**, disponível em: <https://www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-due-diligence-e-novos-negocios-06082020#_ftn3>, acesso em: 27 Set. 2021.

Declaração Universal dos Direitos Humanos. Unicef.org. Disponível em: <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>>. Acesso em: 20 Maio 2021.

Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 2... - EUR-Lex. Europa.eu. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>>. Acesso em: 21 Maio 2021.
DONEDA, Danilo.

FALEIROS Júnior, José Luiz De Moura ; MARTINS, Guilherme Magalhães, **Proteção de dados e anonimização: perspectivas à luz da lei nº 13.709/2018, rei - revista estudos institucionais**, v. 7, n. 1, p. 376–397, 2021.

FONTES, E. L. G.. **Segurança da Informação: o usuário faz a diferença**. São Paulo: Saraiva, 2006.

GOMES, Maria Cecília Oliveira. **Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD**. Disponível em https://www.academia.edu/41160034/Relat%C3%B3rio_de_Impacto_a_Prote%C3%A7%C3%A3o_de_Dados_Pessoais_uma_breve_an%C3%A1lise_da_sua_defini%C3%A7%C3%A3o_e_papel_na_LGPD.

DATE, C.J. **Introdução a sistemas de bancos de dados**. 8º ed. Rio de Janeiro: Gen. 2004

Lei Geral de Proteção de Dados entra em vigor, Senado Federal, disponível em: <<https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>>, acesso em: 3 Jun. 2021.

LETÍCIA, Antunes; TAVARES; ACOSTA ALVAREZ, Bruna, **Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil**, [s.l.]; [s.d.], disponível em: <<https://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas.>>, acesso em: 3 Jun. 2021.

MELO, Celso Antônio Bandeira. **Curso de Direito Administrativo**. 26 ed. São Paulo: Malheiros. 2009

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: www.revistadir.ufv.br. Saraiva, 2014.

MENDONÇA, José Xavier Carvalho de. **Tratado de direito comercial brasileiro. atualizado por Ricardo Negrão**. Campinas: Bookseller, 2000. V. 1

O Guia de Elaboração de Termo de Uso e Política de Privacidade para Serviços públicos. Brasília, Junho de 2021.

Revista de Doutrina da 4ª Região, Trf4.jus.br, disponível em: <https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html>, acesso em: 20 Maio. 2021.

RIBEIRO, Maisa de Souza. **Due diligence para identificar e medir passivos ambientais.** Revista Trevisan. 2001.

RUARO, Regina Liden. GLITZ, Gabriela Pandolfo Coelho. **Panorama Geral Da Lei Geral De Proteção De Dados Pessoais No Brasil e a Inspiração No Regulamento Geral De Proteção De Dados Pessoais Europeu.** REPATS, Brasília, V.6, nº 2, p 340-356, Jul-Dez, 2019.

SCHREIBER, Anderson. **Marco Civil da Internet: Avanço ou Retrocesso? A Responsabilidade Civil por Dano derivado do Conteúdo Gerado por Terceiro.** [s.l.]: , [s.d.]. Disponível em: <<http://www.andersonschreiber.com.br/downloads/artigo-marco-civil-internet.pdf>>. Acesso em: 21 Maio 2021

Sobre a Lei de Acesso à Informação, CAPES, disponível em: <<https://www.gov.br/capes/pt-br/acesso-a-informacao/servico-de-informacao-ao-cidadao/sobre-a-lei-de-acesso-a-informacao>>, acesso em: 3 Jun. 2021

TEPEDINO. Gustavo, TEFFÉ, Chiara Spadaccini de. **O consentimento na circulação de dados pessoais.** 2020

VICTORIA, Maria ; KRIEGER, Antunes, **universidade federal de santa catarina centro de ciências jurídicas curso de graduação em direito**, [s.l.: s.n., s.d.]. Acesso em: 21 Maio 2021.

ZANON, João Carlos. **Direito à proteção dos dados pessoais.** São Paulo: Revista dos Tribunais, 2013.