LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: Desafios e conquistas do Brasil

Rafael Pedro Souza de Freitas[1]

Michele Cia[2]

RESUMO: O presente trabalho aborda temas da Lei Geral de Proteção de dados brasileira. A Lei Geral de Proteção de Dados, inspirada na lei Europeia *General Data Protection Regulation,* tem como finalidade a tutela dos direitos das pessoas naturais, por meio do tratamento de dados que pessoas naturais e jurídicas conferem a dados pessoais. A relevância deste trabalho se justifica pela importância da proteção de dados que são um direito fundamental. A LGPD aborda principalmente o direito à privacidade, violado constantemente no mundo digital. A LGPG além de trazer diretrizes para o tratamento de dados, também criou o profissional *Data Protection Officer,* profissional importante para a implementação da política de dados nas empresas, que possui destaque no presente trabalho, por ser aquele personagem principal para a aplicação efetiva da lei. Utilizou-se o método científico de pesquisa exploratória para a realização deste trabalho, onde foi possível analisar artigos científicos, doutrina e legislação acerca do tema.

Palavras-chave: Direito Digital**,** Dados Pessoais, Lei Geral de Proteção de dados, informática.

SUMÁRIO: 1. Introdução; 2. Teoria da Virtualidade e da Atualidade e Cyberspace; 3. Proteção de dados, um direito fundamental; 4. Modelo Europeu de proteção de dados; 5. *Data Protection Officer*; 6. Considerações finais; 7. Referências.

1. INTRODUÇÃO

O Brasil inaugurou com a lei 13.709, de 14 de agosto de 2018, o marco civil da proteção de dados pessoais. A referida lei conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foi sancionada pelo Presidente Michel Temer em agosto de 2018, mas entrará em vigor no ano de 2020. O objetivo principal da legislação é regulamentar a forma como os dados pessoais de clientes e usuários

[1]Discente do 10º período do curso de Direito da Libertas Faculdades Integradas e Graduado em Sistemas de Informação pela Libertas Faculdades Integradas. E-mail: ledzepedro@gmail.com
[2]Coordenadora e Docente do curso de Direito da Libertas Faculdades Integradas

são utilizados por parte de empresas públicas e privadas. Conforme o texto do artigo primeiro da própria lei:

> Art. 1º Esta 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 (BRASIL, 2018)

Em linhas gerais o tratamento de dados é o processo de utilização de dados pessoais, tais como a coleta, a classificação, a utilização, o processamento, o armazenamento, o compartilhamento, a transferência, a eliminação, entre outras ações realizadas com os dados de pessoas jurídicas e físicas.

A LGPD também conceitua diversos termos que são utilizados no procedimento de tratamento de dados. O artigo 5° com seus incisos realizam esse papel. Como por exemplo o conceito de "*I-dado pessoal: informação relacionada a pessoa natural identificada ou identificável*", e "*IV- banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico"* (BRASIL, 2018).

A lei também criou órgão fiscalizador que é a Autoridade Nacional de Proteção de Dados, segundo a Agencia Brasil:

> A fiscalização ficará a cargo da Autoridade Nacional de Proteção de Dados (ANPD). Após vetos, uma Medida Provisória (No 869 de 2018) editada e aprovada (na forma da Lei No 13.353 de 2019) mudando a Lei e novos vetos pelo presidente Bolsonaro, a Autoridade perdeu poderes frente ao previsto na primeira redação da Lei aprovada pelo Congresso em 2018. Diferentemente da versão do Parlamento, o órgão não terá uma estrutura independente, mas ficará subordinado à Presidência da República, com um compromisso de revisão de sua natureza institucional após dois anos (VALENTE, 2019).

O Brasil atualmente não possui legislação de proteção de dados, o que deixa uma vulnerabilidade gigantesca para ataques cibernéticos. Á título de exemplo nos últimos anos, o uso indevido de cadastros financeiros de consumidores provocou um número enorme de reclamações. Conforme levantamento feito pelo Instituto Brasileiro de Defesa do Consumidor (IDEC), reclamações envolvendo problemas com transparência e uso inadequado de dados pessoais cresceram 1.134% entre 2015 e 2017. A principal queixa, com 63% dos apontamentos, é

referente à publicação, consulta ou coleta de dados pessoais sem autorização do consumidor (REUTERS, p. 3)

A proteção de dados é extremamente importante para um país. Diversas nações estão revendo os seus conceitos e legislações acerca da proteção de dados pessoais. No ano passado a União Europeia colocou em vigência lei pioneira de proteção de dados pessoais e a privacidade. O que era de se esperar já que os escândalos de vazamento de dados de grandes empresas ficaram mundialmente conhecidos, gerando assim grande discussão acerca do assunto.

No caso da Europa, diferentemente do Brasil, já existia legislação vigente desde 1995, mas a nova lei foi imprescindível para estabelecer uma nova dinâmica de uso de dados da rede, haja vista a consolidação de grandes empresas baseadas exclusivamente na internet.

O presente trabalho busca analisar a necessidade da criação da legislação brasileira de proteção de dados, para explanar entendimento acerca dos desafios e compromissos criados a partir da legislação.

O estudo e desenvolvimento deste tema é de grande relevância, já que diversas empresas brasileiras, o próprio governo brasileiro terá impacto a respeito da maneira como lida com os dados pessoais. O estudo e discussão acerca da legislação que entrará em vigor fortalecerá os seus termos e enriquecerá a doutrina do tema. Neste sentido, o trabalho a ser desenvolvido, esta devidamente atualizado com a evolução legislativa brasileira, e acompanhará o seu trajeto de implantação, buscando investigar, a sua trajetória de construção, ativação e resultado.

2. TEORIA DA VIRTUALIDADE, ATUALIDADE E CYBERSPACE

Aquilo que é virtual existe como potência e não como um ato. Aquilo que é virtual não é o contrário do que é real, mas sim oposição à atualidade, “*a virtualidade e a atualidade são duas maneiras de ser distintas*”. Para o filósofo Pierre Lévy, em sua obra *Sur les Chemins du Virtuel,* a antonímia entre os conceitos de real e virtual não são válidos quando aplicados no entendimento do espaço digital. Para o filósofo o virtual não se opõe ao real, mas sim ao atual (LIMA; PEROLI, 2019, p. 19; LÉVY, 1995, p. 3).

> A virtualidade é uma potencia que acompanha uma realidade atual e que a convoca a uma atualização, que é a criação de uma ideia ou forma a partir de uma potência (o virtual) (LIMA; PEROLI, 2019, p.19).

Ainda buscando o entendimento do filósofo Pierre Lévy aquilo que se considera possível já se encontra em estado constituído como real, mesmo que não esteja no plano da realidade, pode ser realizado. Fazer com que o possível se torne real não é uma criação, já que a criação implica na inovação de uma ideia ou forma. "*Contrariamente ao que já é constituído, seja o real ou o possível, o virtual é um conjunto de forçar (uma potência) que acompanha um problema e que o conclama a uma resolução: uma atualização*"((LIMA; PEROLI, 2019, p. 19; LÉVY, 1995, p. 3).

O desenvolvimento de um *software* acontece quando se tem a junção do real com a potência do virtual, sendo que a influência mútua entres os humanos e a informática a "*dialética do atual com o virtual*". Os programadores - profissionais da área de desenvolvimento de *softwares* – ao construírem um programa enfrentam problemas originais, podendo cada profissional chegar a diferentes soluções, por diferentes meios.

> Essas atualizações podem qualificar ou desqualificar competências, solucionar ou desencadear conflitos, como instaurar novas situações, porque os *softwares* trazem em si, como realidade atual, uma virtualidade para mudanças, que é a potência à atualização. A atualização é uma reposta à virtualidade (LIMA; PEROLI, 2019, p. 20).

A atualização pode ser entendida como a caminhada de um problema para a sua solução, já a virtualização é a caminhada de uma solução para outro problema, que modifica a atualidade inicial para um problema particular.

Destaca-se que para o entendimento da proteção de dados e as suas aplicações a diferenciação entre a teoria da virtualidade da atualidade são relevantes justamente para a questão normativa do tema da proteção de dados e dos efeitos tecnológicos que toda a cadeia da internet e *web*, trouxeram no espaço-tempo pela agilidade das atualizações. Nesse mesmo sentido entender, ainda que brevemente o conceito do termo *Cyberspace,* é de grande relevância.

O termo *cyberspace* tem origem advinda de Pierre Lévy, que conceitua conforme a sua derivação do latim *virtualis.* O *Cyberspace* é um considerado transcendente às experiências da internet, não podendo ser considerado somente

um meio de comunicação digital, mas um espaço que compreende uma nova forma de vida e cultura social (LIMA; PEROLI, 2019, p. 22-23).

Em 1996, John Perry Barlow, criou a Declaração de Independência do *Cyberspace*, onde abordou o tema com liberalidade, defendendo a sua independência de normas de direito e de ausência de fronteiras, que foi estruturado por um contrato social assumido por seus usuários. Já o século XXI trouxe limitações a liberdade do *Cyberspace*. A sociedade acabou levando os conflitos reais que possuíam ao espaço e até mesmo criou outros. Nesse sentido, outros especialistas no tema, como Joel Reildenberg, propuseram a autorregularão do espaço digital, sendo de suma importância. Em sua obra Reildenberg propôs que a ausência de tratamento do conteúdo no espaço digital, tratamento dos dados pessoais e a preservação dos direitos de propriedade, poderiam incorrem em conflitos entre países (LIMA; PEROLI, 2019, p. 24).

Nesse contexto o espaço digital necessita de estabilidade e de confiança para que possa ser utilizado por toda a sociedade. O *Cyberspace* já se consolidou como um meio de informação, sejam estas confiáveis ou não e justamente no sentido de trazer mais credibilidade ao que é propagado ali, a regulamentação deste deve ser cogitada. A propagação de *Fake News,* dados privados, em contrapartida a ao direito à privacidade e propriedade são temas que corriqueiramente estamos lidando, por tanto a regulamentação do *Cyberspace* é indiscutível. Assim passamos a analisar a necessidade da proteção dos dados.

1. PROTEÇÃO DE DADOS, UM DIREITO FUNDAMENTAL

A fim de valorar o direito a proteção de dados é necessário abarcar o tema do direito à privacidade que todo cidadão possui. Quando cogitamos um direito fundamental a proteção de dados, este está intimamente ligado a investigação sobre as dimensões do conceito de privacidade, haja vista que a construção de uma nova infraestrutura social, nascida com o advento da Internet, representa uma Segunda Revolução das Comunicações. Atualmente podemos classificar a sociedade como uma sociedade das informações, e sendo a informação a célula principal da composição da estrutura da sociedade. Diante de tamanha importância o tratamento de dados é de grande relevância (MARTINS, JÚNIOR; 2019, p. 53-54).

Tamanha a importância do tema aqui estudado que atualmente o Brasil possui em tramitação no Congresso Nacional a Proposta de Emenda à Constituição número 17 de 2019, que trata quer acrescentar um inciso ao artigo 5° e um inciso ao artigo 22 para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e ainda ficar a competência privativa da União para Legislar sobre o tema.

Nota-se que a Constituição Federal Brasileira de 1988, embora jovem, com relação ao tema em discussão não prevê a proteção dos dados, o que pode ser justificado pelo avanço repentino e voraz que a internet trouxe ao país após a sua promulgação.

Na justificação da PEC 17/2019, o Senador Eduardo Gomes destaca que o avanço da tecnologia cria mecanismos para que negócios e a própria atividade econômica são capazes de gerar prosperidade, empregos, qualidade de vida e meios integração social, entretanto a falta de regulamentação legal pode representar riscos às liberdades e garantias individuais do cidadão.

Além da PEC 17/2019 o Brasil possui outras legislações já em vigência que preveem algum tipo de proteção de dados, como por exemplo sigilo dos agentes fiscais prevista no Código Tributário Nacional, sigilo da gravação ambiental, lei 105/2001 que trata do sigilo bancário, entre outras. Contudo essas legislações são específicas e não possuem um alcance normativo amplo, no sentido de considerar o direito à privacidade como direito fundamental autônomo. Desta forma o acúmulo de informações que particulares e até mesmo o estado mantém como o registro, o uso, a análise, a combinação e algumas vezes a exposição dessas informações ameaçam a privacidade dos cidadãos (MARTINS, JÚNIOR; 2019, p. 58).

A LGPD inspirada na *General Data Protection Regulation* (GDPR), é uma lei da União Europeia que trata da proteção e dados e identificação dos cidadãos europeus. A LGPD, determina o tratamento de dados pessoais nos setores público e privado com a finalidade de dar proteção aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

O dispositivos da LGPD aplicam-se a quaisquer pessoa natural ou jurídica, de direito privado ou público, que de alguma forma faça o tratamento de dados pessoais, independente do meio – digital ou físico – sendo que esse tratamento ocorra no território nacional, tendo por objetivo oferta ou fornecimento de bens ou serviços, ou tratamento de dados individualizados localizados em nosso país, e os

dados tenham sido coletados no Brasil. Esses requisitos estão presentes no artigo 3° e seus incisos da LGPD (COELHO; LOTUFO; 2019, p. 227).

A LGPD criou quatro titulares de direitos e deveres principais que são o titular, o controlador, operados e encarregado. Sendo que cada um desses tem um papel importante imposto pela lei. Conforme Fábio Ulhoa Coelho e Mirelle Bittencourt Lotufo:

> O *titular* dos dados pessoais é a pessoa natural a quem se referem os dados pessoais. O controlador é a sociedade ou pessoa natural que coleta os dados pessoais e a quem compete as decisões referentes ao tratamento de dados pessoais. O operador, é também sociedade ou pessoa natural, que realiza o tratamento de dados pessoais em nome do controlador. Por fim, o encarregado é a pessoa natural, indicada pelo controlador, que atua como canal de comunicação de qualquer fato relevante sobre tratamento de dados (2019, p. 227).

O artigo 5°, inciso X, da LGPD define o que é o tratamento dos dados pessoais, sendo toda operação realizada com as informações de um ou mais indivíduos, sendo essas informações com diversos conteúdos como idade, gênero, religião, profissão, estado civil, CPF, perfil de consumo, entre outros. O inciso X determina todas as ações que configuram o tratamento:

> 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;

Nota-se que o tratamento de dados irá atingir diversos setores da sociedade, como por exemplo campanhas publicitárias que coletam dados para pesquisa, pesquisa de mercado, publicas ou privadas, programas de fidelização de clientes, realização de pesquisas pelo poder público para a formulação de políticas públicas mais condizentes com a realidade, etc (COELHO; LOTUFO; 2019, p. 227).

Destaca-se que a LGPD prevê algumas exceções no tratamento de dados pessoais, e elenca essas exceções em seu artigo 4°:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> ~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;~~

> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) (BRASIL, 2018)

A LGPD divide os dados em três classificações, que são os dados pessoais, dados sensíveis e dados anonimizados. Os dados pessoais são aqueles dados relacionados as pessoas naturais identificadas ou identificáveis, como por exemplo: número do Cadastro de Pessoa Física, endereço residencial, número de telefone, etc. Os dados sensíveis são informações relativas à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, informações de saúde ou relativa a vida sexual, dados genéticos ou biométricos. Os dados anonimizados são aqueles dados que não podem ser associados a pessoas naturais, são aqueles que o titular não pode ser identificado. Originalmente esses dados eram relativos a alguma pessoa, mas após passar por etapas de processamento desvinculou-se totalmente da pessoa, sendo impossível identifica-la. Destaca-se que somente se considera dado anonimizado se por meios técnicos de não seja possível reconstruir o caminho para identificar o titular, caso isso seja possível, o dado não será anonimizado e estará sob proteção da LGPD, haja vista que os dados anonimizados não estão sujeitos a LGPD.

> O processo técnico denominado de “anonimização” (artigo 5°, IX, da LGPD) nada mais representa do que a dissociação entre determinado dado pessoal e o seu respectivo titular, Há inúmeros procedimentos específicos que podem ser implementados para a concretização desta meta, quase sempre a partir da supressão de determinados elementos identificadores que constam de uma base de dados, por meio de supressão do dado, generalização, randomização ou pseudoanonimização (MARTINS; JÚNIOR, 2019, p. 61).

Com relação a anonimização do dado, o que se tem é que o grau de identificabilidade deste dado que irá determinar se este pode ser considerado anonimizado ou não. Conquanto, os dados anonimizados são importantes para o desenvolvimento da inteligência artificial, análise de comportamentos, aprendizados das máquinas entre outros, em contrapartida parte da doutrina que estuda o tema da anonimização alertam sofre os riscos da possibilidade da confiabilidade e higidez dos processos técnicos da anonimização de dados (MARTINS; JÚNIOR, 2019, p. 70).

Diante de todo o conteúdo ligado aos dados cabe aqui uma análise dos profissionais que tratam esses dados que será realizada no tópico abaixo.

2. MODELO EUROPEU DE PROTEÇÃO DE DADOS

Mesmo antes do tratado de Maastrich, instituir a União Europeia, em 1993, o mundo e também o Brasil, já era influenciado pelo modelo de direito europeu. Com relação a proteção de dados não foi diferente. A legislação LGPD foi totalmente influenciada pela RGPD da União Europeia (LUCCA; MACIEL, 2019, p. 30).

Os estudos mais importantes da área de proteção de dados surgiram na Europa nos anos 80, principalmente a partir de documentos ordenados por organismos internacionais, como as “*Guideline on the protection of privacy and transborder flows of person data*” , da Organização para Cooperação e Desenvolvimento Enomico (OCDE), e ainda pela Convenção sobre Proteção de Dados pessoais, n° 108, de 28 de janeiro de 1981 (LUCCA; MACIEL, 2019, p. 31).

No ano 1995 editou-se a Diretiva 95/46/CE elo Parlamento e Conselho Europeu para disciplinar a proteção de dados pessoais, onde incentivo para fomentar relações mais próximas entre os Estados que pertencem a União, assegurando o progresso econômico e social , permitindo a livre circulação de dados

pessoais, sendo respeitadas para tanto as liberdades e direitos fundamentais. Também coaduna neste sentido RGDP (LUCCA; MACIEL, 2019, p. 31).

No ano de 2002 a Diretiva 95/46/CE ganhou um reforço da Diretiva 58. A Diretiva 58 que trata do tratamento de dados pessoais voltados à privacidade de dados no conjunto das comunicações eletrônicas, ficando conhecida como "*ePrivacy Diretive*". A partir da *ePrivacy Diretive* houve uma preocupação com limite a coleta, armazenamento e à utilização de dados, naquele contexto de comunicação eletrônica, vindo, portanto a positivar o Princípio da Finalidade, previsto tanto na Lei Europeia, quando na Brasileira (LUCCA; MACIEL, 2019, p. 32).

Nos anos seguintes outras Diretivas Europeias foram surgindo, como a Diretiva 2006/24/CE que alterou o conteúdo da Diretiva 58, que veio para tentar equilibrar as disposições dos Estados-Membros da União Europeia, na tentativa de garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves(LUCCA; MACIEL, 2019, p. 33).

Ainda pautando na evolução da legislação europeia, Lucca e Maciel (2019, p. 33) afirmam que:

> Seguiu-se a Diretiva 2009/136/CE, que acrescentou a Diretiva 2002/58/CE regras sobre serviços universais de comunicação e as redes sociais, destacando-se a exigência de consentimento expresso do indivíduo para o armazenamento das informações e o direito de retirá-lo quando quiser. Além disso, a diretiva 2009/136/EC regulamentou o uso de *Cookies*, tanto que ficou conhecida como "*Cookies Diretive*"

Diante de toda a evolução das legislação europeia sobre a proteção de dados, ficou claro que a Diretiva 95/46/CE já não era capaz de acompanhar com a mesma velocidade a constante evolução tecnológica, assim surgiu a necessidade de instauração de uma legislação que fizesse jus ao tema de uma maneira global e eficiente. A partir daí instaurou-se debates que findaram na atual edição do Regulamento (UE) 2016/679, do Parlamento e do Conselho, de 27 de abril de 2016, conhecido como Regulamento Geral sobre a Proteção de dados – RGPD, conhecida no Brasil como "*General Data Protection Regulation*" – GDPR, que entrou em vigor em 25 de maio de 2018.

Ainda citando os autores Lucca e Maciel (2019, p. 34), acerca da finalidade da GDPR:

> Tal diploma cria, entre outras coisas, a obrigatoriedade de designar um encarregado sobre a proteção de dados; refunda o conjunto de regras a respeito da obtenção do consentimento; elimina o sistema de notificações

> e autorizações; implementa o direito ao esquecimento e impõe multas de valor muito elevado para o descumprimento de suas normas, extremamente agravadas na hipótese de reincidência.

Portando o modelo europeu de proteção de dados é um exponencial no ramo, e dita diretrizes não somente para os países de seu bloco geopolítico, mas também dita condutas que empresas de outros países devem seguir para que eventualmente possam transferir dados entre si. Fica evidente que a LGPD brasileira foi inspirada na GDPR, resguardadas as suas diferenças.

3. *DATA PROTECTION OFFICER*

Conforme mencionado no tópico acima a LGPD criou quatro personagens, titulares de direitos e deveres, contudo analisaremos o papel do Encarregado de Proteção de Dados ou *Data Protection Officer*, conhecido pelo acrônimo DPO. A figura do DPO não foi uma inovação trazida pela LGPD, na realidade como toda a LGPD foi inspirada na GDPR, o DPO também o foi, porém com algumas alterações.

O DPO tem um papel fundamental na aplicação pratica da LGPD. Ele é o profissional que a lei criou que irá orientar a empresa e seus funcionários acerca das regras de tratamento de dados que esta terá de seguir. Destaca-se que esta função é totalmente inovadora no Brasil, o que até mesmo dificulta as empresas em encontrarem pessoa capacitadas para exercerem essa profissão. Ressaltamos ainda que até mesmo na busca por encontrar materiais didáticos, como artigos, doutrinas, e livros acerca desta profissão houve certa dificuldade, justamente pela inovação deste ramo.

A LGPD determina no parágrafo 2° do artigo 41, as atividades que o DPO deverá exercer, cabendo aqui transcrição:

> § 2º 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. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados (Brasil, 2018).

A LGPD não determina que o profissional DPO necessite de formação específica, de cursos ou graduação na área de Tecnologia da Informação, mas o que se tem de consenso é que o profissional DPO deverá ter conhecimento tanto na área de Tecnologia da Informação, quanto na área do Direito, já que uma de suas funções será trabalhar diretamente com o Relatório de Impacto à Proteção de Dados Pessoais, previsto no artigo 38 da LGPD.

O Relatório de Impacto à Proteção de Dados Pessoais contém a descrição das atividades de processamento de dados que podem gerar riscos aos titulares de ados, além de informações sobre a implementação as medidas e instrumentos para diminuírem os danos (MIRANDA, 2019, p. 16).

Segundo Miranda:

> O EPD (semelhante `a figura do DPO – *Data Protection Officer*, previsto na regulacão europeia) é a pessoa natural, nomeada pelo controlador (empregado ou contratado externamento), que atuará como um canal de comunicação entre este, os titulares dos dados e a autoridade de proteção de dados. Será responsável por receber reclamações e comunicações de titulares e órgãos competentes, prestar esclarecimentos, adotar providências e orientar funcionários sobre as boas práticas, dentre outras atribuições. Sua identidade e informações de contato deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no site do controlador. Por não fazer nenhum ressalva específica, a análise da LGPD leva ao entendimento de que qualquer entidade que processe dados pessoais deverá, sob quaisquer circunstâncias, indicar um EPD, cabendo, porém, a autoridade nacional estabelecer normas complementares sobre a definição e a atribuição da pessoa responsável (incluindo hipóteses de dispensa de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados) (MIRANDA, 2019, p. 13).”

Merece destaque o profissional de TI perante a LGPD. Conforme já mencionado a LGPD determina maneiras de gerenciar os dados coletados, que quase sempre são processados por meio de sistema da computação, ou seja, ficam sob a responsabilidade do setor de tecnologia das empresas. Dessa forma o profissional de tecnologia da informação deve estar alinhado com o conteúdo e exigências da LGPD (MIRANDA, 2019, p. 17).

Todo o setor de tecnologia da informação deverá oferecer ferramentas de segurança ainda mais fortes para auxiliar na segurança dos dados tratados, protegendo assim contra ataques, bem como proceder com transparência em suas ações, para que os clientes saibam como seus dados estão sendo protegidos, “*o profissional desse setor será o responsável por cuidar dos backups, das medidas de*

segurançaa, da atualização dos softwares e integraçãoo de informações.”(MIRANDA, 2019, p. 17).

5. CONSIDERAÇÕES FINAIS

Diante de todo o desenvolvimento do trabalho foi possível verificar a importância do tema para a vida de todas as pessoas que utilizam os mais variados meios de tecnologia, principalmente para as empresas que atuam diretamente na coleta de dados. Verificamos que a sociedade, movida a informação impõe a necessidade de controles contra a atividade exploratória e abusiva de coleta e dados e informações, e diante dessa necessidade surgiu a LGPD, mais um mecanismo de proteção de dados.

Pautando nossos estudos da teoria da virtualidade e no conceito de *Cyberspace* entendemos que o existe um novo ambiente de convivência em sociedade, que se comunica constantemente, troca informações, serviços, gera cultura, ou seja, um ambiente que reproduz a vida em sociedade, e portanto deve ter alguma regulação para que os direitos fundamentais dos seus usuários não sejam violados.

Buscamos ainda entendimento do direito fundamental a proteção de dados e privacidade nesse novo ambiente virtual. O presente trabalho demonstrou a importância da proteção de dados, por meio da Proposta de Emenda à Constituição número 17 de 2019, que quer acrescentar um inciso ao artigo 5° e um inciso ao artigo 22 para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e competência privativa da União para Legislar sobre o tema.

Outrossim, analisamos a LGPD, que foi inspirada na *General Data Protection Regulation* (GDPR), lei da União Europeia que trata da proteção e dados e identificação dos cidadãos europeus. Buscamos os dispositivos que tratam diretamente do tema e os conceitos dos tipos de dados que a lei inaugura. Ainda analisamos brevemente os personagens que a lei cria titulares de direitos e deveres, dando destaque ao DPO, profissional que deverá ter conhecimento tanto na área da tecnologia da informação quanto na área do direito.

A partir do breve estudo do desenvolvimento da GDPR concluímos que a LGPD buscou pautar-se nas diretrizes daquela, utilizando como inspiração seus

principais princípios e objetivos. Nesse sentido um dos principais personagens trazidos pela GDPR e reproduzido pela LGPD é o *Data Protector Officer*. Este profissional é o responsável pela implementação da política de dados das empresas e órgãos sujeitos a LGPD. O DPO possui grande responsabilidade, e deve ter conhecimento tanto na área das ciências exatas, no trato com a tecnologia da informação, quanto na área das ciências humanas, no trato com o direito aplicado pela lei.

Todo o trabalho, buscou demonstrar uma realidade que a sociedade toda enfrenta que é a virtualização dos dados e informações. A inteligência artificial caminha a passos avançados na busca de evolução e o direito deve sempre estar ao lado, senão a frente desta caminhada, para que os princípios e direitos fundamentais não sejam violados. A LGPD veio como uma ferramenta para a proteção desses direitos, e ainda que alguns tenham críticas quanto aos seus dispositivos, a importância de sua existência não pode ser questionada.

6. REFERÊNCIAS

BRASIL. Lei n° 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial [da] República federativa do Brasil**, Brasília, DF, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 15 set 2019.

BRASIL. Proposta de Emenda à Constituição n° 17 de 2019. Brasília, DF: Senado Federal, [2019]. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1594003895291&disposition=inline> Acesso em: 01 de set. 2020.

LÉVY, Pierre. **Sur les Chemins du virtuel**. Paris: UNiversité Paris-8 St. Denis, 1995, Disponível em: <http://www.manuscritdepot.com/edition/documents-pdf/pierre-levy-le-virtuel_01.pdf> . Acesso em: 09 set. 2020

LIMA, Cíntia Rosa Pereira; KELVIN Peroli. Direito Digital, Conpliance, Regulamentação e Governança. **Quartier Latin**, São Paulo, 2019.

LUCCA, Newton De; MACIEL, Renata Mota. A lei n° 13.709, de 14 de Agosto de 2018: A Disciplina Normativa que Faltava. In: **Direito em internet IV: Sistema de Proteção de Dados Pessoais**. Quartier Latin, São Paulo, 2019, p. 21-51.

LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira; MACIEL, Renata Mota. Direito em internet IV: Sistema de Proteção de Dados Pessoais. **Quartier Latin**, São Paulo, 2019.

MARTINS, Guilherme Magalhães; JÚNIOR, José Luiz de Moura Faleiros. A Anonimização de Dados Pessoais: Consequências Jurídicas do Processo de Reversão, a Importância da Entropia e sua Tutela à Luz da Lei Geral de Proteção de Dados. *In*: LUCCA, Newton De; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (org). **Direto & *Internet IV* Sistema de Proteção de Dados Pessoais**. 1 ed. São Pulo Quartier Latim, 2019.

MIRANDA, Marcelo Gonçalves: Lei Geral de Proteção de Dados - LGPD. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/60614977/LGPD20190916-13654-1541n4r.pdf?1568655695=&response-content-disposition=inline%3B+filename%3DLei_Geral_de_Protecao_de_Dados_LGPD.pdf&Expires=1599836303&Signature=Zzd8A6Ir63fecpQ8i60XMlXVUjU1HyNPjGVX7kLL1BbS8tMDbxoc4rmBuABd1vJhnirCMdDvxhrYy7rgSmEnBTv6ikRjM24EGdgVJtLFybNYocyFITngoHiva01oLv9mM~dLogosrdKVUObQLWMT9CkkLwOayBiJ2Ft1GA3-64wTjJSPI0ofZrli8eDlQdD~kx8JYO0OWkRvTG857~tGf2Q~tbpNmhIecoFXKKct3YslMol0ZNtBN5Oh2uzgTLB3MN44bTWLqqGJo35Fz7IFnH0mRL1jtI-1BYW6jsJDofw6pVUBRgnIMXuZGYE8MKrXWno190r44jWX3Wyr4PvB0A__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA Acesso em: 05 de ago. 2020.

NORONHA, Laura Almeida. criação do data protection officer interpretado á luz da lei geral de proteção de dados pessoais. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7815/67648479> Acesso em: 05 ago. 2020.

THOMSON REUTERS. **Lei Geral de Proteção de Dados: impactos e mudanças no uso e na coleta de dados pessoais**. Disponível em: <https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/thomson-reuters-legal-whitepaper-lei-geral-de-protecao-de-dados.pdf> Acesso em: 14 set. 2019.

VALENTE, Jonas. Lei de Proteção de dados traz desafios a empresas, cidadãos e governo. **Agência Brasil**, Brasília, 25 ago. 2019. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo> Acesso em: 13 set. 2019.