UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES
PRÓ-REITORIA DE ENSINO, PESQUISA E PÓS-GRADUAÇÃO
CAMPUS DE ERECHIM
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

MICHELE PUERARI

A LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES JURÍDICAS: UM ENSAIO SOBRE O ANONIMATO E O DIREITO À PRIVACIDADE

ERECHIM
2021

MICHELE PUERARI

A LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES JURÍDICAS: UM ENSAIO SOBRE O ANONIMATO E O DIREITO À PRIVACIDADE

Monografia Jurídica apresentada para obtenção do título de Bacharel em Direito no Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões – Campus de Erechim.

Orientadora: Prof.ª M.e Simone Gasperin de Albuquerque

ERECHIM
2021

MICHELE PUERARI

A LEI GERAL DE PROTEÇÃO DE DADOS E SUAS IMPLICAÇÕES JURÍDICAS: UM ENSAIO SOBRE O ANONIMATO E O DIREITO À PRIVACIDADE

Monografia Jurídica apresentada para obtenção do título de Bacharel em Direito no Curso de Direito do Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões – Campus de Erechim.

_____, ____de _____ de 2021.

BANCA EXAMINADORA

_____
Prof.ª M.e Simone Gasperin de Albuquerque
Universidade Regional Integrada do Alto Uruguai e das Missões

_____
Prof.
Universidade Regional Integrada do Alto Uruguai e das Missões

_____
Prof.
Universidade Regional Integrada do Alto Uruguai e das Missões

Dedico este trabalho à minha família, com todo meu amor.

AGRADECIMENTOS

Diante de todo o esforço para que o presente trabalho fosse concluído, não poderia deixar de mencionar o meu carinho por algumas pessoas que fizeram parte de toda a minha trajetória acadêmica e que de alguma forma, são especiais para mim.

Inicialmente agradeço a Deus pela vida, por toda força, saúde, ânimo e coragem oferecidos para as dificuldades serem superadas e essa meta alcançada.

Aos meus pais, Marlene e Claudio, a quem eu devo tudo. Aqueles que fizeram e continuam fazendo absolutamente tudo valer a pena. Toda minha gratidão pelo apoio emocional e financeiro, pelo amor, carinho, respeito, educação e por não medirem esforços para que eu pudesse realizar este sonho. Serão meus alicerces para toda a vida. Sou imensamente grata por ter vocês.

Ao meu irmão, Silvan, por ser o meu “espelho” e pelo apoio prestado nesse período.

Ao meu namorado, Leonardo, pelo carinho e por sempre acreditar em mim. Obrigada pelo amor e pela paciência.

À minha orientadora Prof.ª M.e Simone, por toda a atenção, carinho e pela disposição prestada mesmo em época de pandemia, por sempre estar presente para indicar a direção correta que o trabalho deveria tomar. Gratidão por todos os ensinamentos e pelas valiosas contribuições dadas durante todo esse processo.

À todos os professores que fizeram toda diferença na minha formação e são exemplos de profissionais.

À todos os colegas da turma, Felipe, Silvia, e em especial minha amiga e colega Ana Claudia, por sempre me incentivar e por estar desde o início da faculdade presente em todos os momentos, motivando e ajudando. Se tornou especial com seu “espírito revolucionário”, aceitando mudar o mundo comigo em um minuto.

Por fim, agradeço de forma singela, a todos que estiverem presentes nessa jornada e que me motivaram de alguma forma.

"Tudo está fluindo. O homem está em permanente reconstrução; por isto é livre: liberdade é o direito de transformar-se".

Lauro de Oliveira Lima

RESUMO

O presente trabalho teve como objetivo a verificação dos limites éticos e jurídicos em relação aos usos de informações pessoais dos usuários de serviços digitais por empresas e autoridades públicas para proteção ao anonimato e o direito de privacidade segundo Lei de Proteção de Dados. Vários fatos contribuíram para uma mudança na realidade social e para um avanço gigantesco do Direito Digital. A interligação física e a uniformização do sistema de transmissão de dados entre as redes permitiram, portanto, que a internet conquistasse maior amplitude. A Lei Geral de Proteção de Dados (LGPD) foi uma iniciativa nacional para estabelecer parâmetros legais aos usos de dados pessoais. Esta regulamentação foi espelhada no Regulamento Geral de Proteção de Dados (GDPR) estabelecido pela Comissão Europeia, e coloca o Brasil na lista de países seguros para a utilização de dados. Traz grandes impactos, uma vez que coleta todos os dados, no território nacional pretende proteger os dados pessoais da população. As técnicas de pesquisa envolveram Pesquisa bibliográfica e pesquisa documental, utilizando-se o método indutivo e analítico-descritivo. A LGPD é um dispositivo que estabelece padrões sobre quais dados de usuários, armazenados por empresas, são pessoais ou sensíveis, além de trazer regras de como eles devem ser tratados e armazenados. A lei dispõe ainda de punições para eventuais descuidos e também fala de uma autoridade nacional para fiscalização.

Palavras-chave: Anonimato. Privacidade. Proteção de Dados. Direito Digital.

ABSTRACT

The present study aimed to verify the ethical and legal limits in relation to the use of personal information by users of digital services by companies and public authorities to protect anonymity and the right to privacy according to the Data Protection Law. The choice of the theme was due to several facts that contributed to a change in social reality and to a gigantic advance of Digital Law. The physical interconnection and standardization of the data transmission system between the networks, therefore, allowed the internet to achieve greater breadth. The General Data Protection Act (LGPD) was a national initiative to establish legal parameters for the use of personal data. This regulation was mirrored in the General Data Protection Regulation (GDPR) established by the European Commission, and places Brazil on the list of safe countries for the use of data. It has great impacts, since it collects all data, in the national territory it intends to protect the personal data of the population. The research techniques involved bibliographic research and documentary research. With inductive and analytical-descriptive method. The LGPD is a device that sets standards on what user data, stored by companies, is personal or sensitive, in addition to providing rules on how they should be treated and stored. The law also provides for penalties for possible carelessness and also speaks of a national authority for inspection.

Keywords: Anonymity. Privacy. Data Protection. Digital Law.

LISTA DE ABREVIATURAS

ANPN	Autoridade Nacional de Proteção de Dados
CF/88	Constituição Federal de 1988
CPC	Código de Processo Civil
GDPR	Regulamento Geral de Proteção de Dados
IP	*Internet Protocol*
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
MP	Ministério Público
OCDE	Organização para a Cooperação e Desenvolvimento Econômico

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho enfoca a questão do direito fundamental à privacidade, dando destaque à proteção e à violação de dados pessoais. Com a evolução tecnológica em um mundo cada vez mais globalizado, a internet e as redes sociais norteiam quase todas as relações individuais. Vivemos em um crescente desenvolvimento tecnológico, e a internet atinge cada vez mais usuários, em busca dos mais diversos bens e serviços, bem como entretenimento e informação.

Nesse cenário de constante crescimento, com a velocidade que os dados circulam na rede e são transmitidos, torna-se cada vez mais difícil acompanhar as atividades humanas que violam interesses pessoais e a vida privada. Problemas como o armazenamento, tratamento, divulgação, comercialização de dados sigilosos de usuários na rede sem a devida autorização, fotos íntimas vazadas na internet, pornografia, anonimato na rede, spam, entre outras violações, contribuem para o aumento de demandas em todas as esferas jurídicas, ensejando indenizações por danos causados pela violação ao direito à privacidade.

Todo indivíduo tem o direito a proteção de suas propriedades e de sua privacidade, estando sobre a ótica da Constituição Federal de 1988. Com essas relações entre pessoas e empresas passam a exigir novas regras, princípios, regulamento e o surgimento de novas leis, como a Lei Geral de Proteção de Dados (LGPD) de 2018, que traz novas práticas que definem como organizações devem cuidar e preservar nossos dados.

A Lei Geral de Proteção de Dados (LGPD) foi uma iniciativa nacional para estabelecer parâmetros legais aos usos de dados pessoais. Esta regulamentação foi espelhada no Regulamento Geral de Proteção de Dados (RGPD) estabelecido pela Comissão Europeia, e coloca o Brasil na lista de países seguros para a utilização de dados. Traz grandes impactos, uma vez que coleta todos os dados, no território nacional, e pretende proteger os dados pessoais da população.

Para tanto, o objetivo geral da monografia foi verificar os limites éticos e jurídicos em relação aos usos de informações pessoais dos usuários de serviços digitais por empresas e autoridades públicas para de proteção e vedação do anonimato e o direito de privacidade segundo A Lei de Proteção de Dados (LGPD).

Para cumprir com o objetivo exposto, esta monografia se divide em três capítulos. No primeiro capítulo abordar-se-á a previsão Constitucional para a

proteção do Direito a privacidade, bem como, sua vedação ao anonimato. Busca-se esclarecer os princípios do direito à privacidade nos tratados de direitos humanos, trazer a evolução histórica da questão da privacidade no Brasil.

Em um segundo momento, o objetivo será apresentar a construção da concepção do Direito Digital, suas características, bem como, a evolução da sociedade digital. Busca-se esclarecer a conceituação do Direito Digital, o uso das redes sociais refletida nessa nova sociedade digital e a promulgação da lei chamada Marco Civil da Internet (MCI) responsável por garantir à informação e a proteção. Por fim, trazer as principais recomendações para blindagem legal das empresas nas redes sociais.

No terceiro e último capítulo será apresentado um avanço importante a Lei Geral de Proteção de Dados (LGPD), bem como, sua aplicabilidade e o cumprimento das normas frente os princípios do direito a privacidade e a vedação do anonimato, trazendo também os principais pontos de um cada um dos capítulos da lei. E por fim, abordar a proteção e tratamento de dados pessoais.

As técnicas de pesquisa envolveram pesquisa bibliográfica e pesquisa documental, utilizando-se o método indutivo e analítico-descritivo.

A relevância do estudo do tema é que em meio a Era Digital, é indispensável abordar sobre regras, uso de dados e de relações jurídicas, provenientes do mundo virtual. É preciso acompanhar a evolução da sociedade no Direito Digital, informar a sociedade quanto à segurança e privacidade de seus dados pessoais ao utilizar esse meio tão tecnológico e dominado por fraudes anônimas.

2 O DIREITO À PRIVACIDADE X A VEDAÇÃO AO ANONIMATO

O presente capítulo tem por objetivo apresentar a previsão Constitucional para a proteção do Direito à privacidade, bem como, sua vedação ao anonimato.

O Direito Digital tem o desafio de equilibrar a difícil relação existente entre interesse comercial, privacidade, responsabilidade e o anonimato, gerado pelos novos veículos de comunicação.

Inicialmente, busca-se esclarecer os princípios do direito à privacidade nos tratados de direitos humanos.

Por fim, trazer a evolução histórica da questão da privacidade no Brasil.

2.1 O DIREITO À PRIVACIDADE E SUA PREVISÃO CONSTITUICIONAL

Todo indivíduo deve ter direito a proteção de suas propriedades e de sua privacidade. Isso é indiscutível. No tocante à propriedade, há tantos bens tangíveis como bens intangíveis. Nesse sentido, suas informações, em última análise, são um ativo de sua propriedade e, portanto, merecem proteção. (PINHEIRO, 2016, p.95)

Observa-se que a Constituição Federal de 1988 (CF/88) protegeu a liberdade de expressão em seu art. 5º, IV, que dispõe: “é livre a manifestação do pensamento, sendo vedado o anonimato;”, mas determinou que seja com “responsabilidade”. (BRASIL, 1988).

Interpreta-se a aplicação da CF/88 em conformidade com o disposto no Código de Processo Civil de 1015 (Lei nº 13.105/2015)[1], em seus artigos. 186 e 187, que determina a responsabilidade por indenizar pelo dano causado, quer quando o ato ilícito tenha sido causado por ação ou omissão, quer quando é fruto do exercício legítimo de um direito qual o indivíduo que o detém ultrapassou os limites da boa-fé e dos bons costumes. (PINHEIRO, 2016, p. 90)

Devido a importância de se garantir o direito à informação e a proteção da liberdade de expressão, foi promulgada uma lei específica no Brasil para tratar de algumas destas questões chamada de Marco Civil da Internet e a Lei Geral de Proteção de Dados que abordarei em outro capítulo.

[1] A lei em comento encontra-se disponível no site: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 14 out. 2020.

A Constituição Federal de 1988 declara como direitos fundamentais do cidadão a inviolabilidade de sua privacidade e intimidade vida privada, a honra e a imagem das pessoas em seu art. 5º, X que dispõe:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindose aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (...). (BRASIL, 1988).

Compreende-se, que qualquer ato, seja ele de natureza tecnológica ou não, é imperioso se ter como escopo o respeito aos princípios constitucionais vigentes. Um dos Princípios enaltecidos na Constituição Federal em vigor está expresso em seu artigo 5.º, XII que preconiza a inviolabilidade da correspondência ou dos dados:

> Art.5.º, XII - É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (BRASIL, 1988).

Situados os direitos à intimidade e à vida privada como direitos fundamentais, e no que toca aos dados que possam ser vetores de ofensas a tais direitos, então pode ser considerada a proteção desses como a forma de garantia a tal direito. (BRASIL, 1988).

Importante destacar que proteção de dados e privacidade são questões diferentes, exemplo de Garcia et al. (2020):

> Se uma pessoa publicar um dado em sua página pessoal numa rede social, ele se torna público. Entretanto, isso não significa que esse dado pode ser utilizado indiscriminadamente. Aquele que vier utilizá-lo, deve respeitar os direitos do Titular do dado, previstos na LGPD. Tais dados, portanto, não estão sob a égide do princípio constitucional da privacidade, mas sim sob o escopo da proteção de dados. (GARCIA et al., 2020, p. 17).

O direito à privacidade constitui um limite natural ao direito à informação. No entanto, não há lesão a direito se houver consentimento, mesmo que implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida. (PINHEIRO, 2016, p. 95).

Atualmente, uma pessoa pode comprar coisas, trocar, usar serviços gratuitos, tudo isso pagando com sua informação. Um valor tão importante quanto a

privacidade é o livre-arbítrio. Por isso a liberdade de contratar entre as partes é fundamental para o democrático-capitalista. (PINHEIRO, 2016 p. 95).

Mas as leis elaboradas no último século, em todo o mundo, foram redigidas sob o manto da proteção a qualquer preço da privacidade do indivíduo, inclusive perante a arbitrariedade do Estado. Assim, nasceram muitas das Constituições Federais. Com artigos dedicados a protegerem o indivíduo da própria coletividade. Direito à intimidade, proteção da reputação de imagem, direito a proteção das informações pessoais e comunicações. (PINHEIRO, 2016, p. 101).

Com certeza o Ministério Público tem um papel fundamental, mas não se impede a pratica do ilícito retirando empresas de operação, mas sim educando os usuários e punindo de forma exemplar quem age errado. Muito pior que o anonimato é o efeito da certeza da impunidade no Brasil. O Marco Civil acabou garantindo a permanecia do conteúdo na internet, atribuindo um peso maior a liberdade de expressão que a proteção da imagem e reputação de um indivíduo na medida em que determina que um conteúdo só seja removido somente após ordem judicial. (PINHEIRO, 2016, p. 104).

Importante destacar algumas dicas para proteger a privacidade:

a) Leia os termos e políticas dos sites antes de cadastrar;
b) Veja se este claro para qual finalidade será usada sua informação e por quanto tempo;
c) Se publicar informação mais pessoal nas redes sociais, faça-o de forma restrita, só para quem você autorizar poder ver e ter acesso;
d) Evite publicar fotos mais intimas;
e) Avalie qual preço você está pagando por um serviço gratuito, seus dados tem valor;
f) Quando cancelar um serviço formalize por escrito (documente) que não quer mais que seus dados continuem a ser usados pela empresa;
g) Faça uma lista de para quem você forneceu dados cadastrais;
h) Oriente seus familiares para evitar publicar suas informações e fotos nas redes sociais sem sua autorização;
i) Em caso de abuso, denuncie. (PINHEIRO, 2016, p. 107-108).

Independentemente dos próximos passos, todo negócio que está na Internet tem que ter uma política de privacidade atualizada, publicada, conteúdo claro, para poder tomar proveito do mercado dos dados sem riscos legais. Ganhará o mercado

quem liderar a proteção da privacidade sustentável com transparência. Até lá, deve-se ler a regra do jogo que está no Termo de Uso dos Serviços antes de aceitar. (PINHEIRO, 2016, p. 107).

Verificou-se neste capítulo que todo indivíduo deve ter direito a proteção de suas propriedades e de sua privacidade protegidos, pois o direito à privacidade constitui um limite natural ao direito à informação. Na sequência serão abordados sobre a previsão Constitucional que veda o anonimato.

2.2 A VEDAÇÃO AO ANONIMATO NA CONSTITUIÇÃO FEDERAL DE 1988

Infelizmente, o anonimato associado à impunidade faz aumentar a agressividade e a violência entre as pessoas dentro da Internet, especialmente no que diz respeito aos crimes contra a honra. A lei brasileira proíbe o anonimato indiscriminado por entender que ele pode gerar danos sociais. Todos têm liberdade de expressão, mas estão sujeitos a responderem por suas declarações. Por isso, devem de identificar. Logo, aqui, o anonimato é uma exceção, quando justificável, e apenas um canal para tanto. (PINHEIRO, 2016, p. 99).

O veto ao anonimato tem a sua abrangência aos meios de comunicação na Constituição Federal de 1988, no art. 5º, IV que dispõe:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: IV - é livre a manifestação do pensamento, sendo vedado o anonimato. (BRASIL, 1988).

Estes envolvem a liberdade de expressão e a garantia da privacidade, do sigilo e dos direitos também previstos por esta. Antes de qualquer coisa e muito óbvia é a intenção da preservação da sua imagem aquele que se prevalece do anonimato, seja ele por ação ou omissão, como hodiernamente ocorre pela internet, essa incógnita recai sobre o nome, a imagem, o endereço físico ou virtual (*e-mail*) e o endereçamento ou número IP (*Internet Protocol*) ou um tipo de “véu” que oculte a real identidade do autor que impossibilite a individualização do transmissor de dados. (BRASIL, 1988).

A promessa da proteção da identidade para estimular a revelação de um conteúdo é algo antigo. Mas os novos aplicativos como o *Secret* desafiam a questão do uso do anonimato para gerar ofensas e ameaças. Patricia Peck Pinheiro, em um

artigo traz o seguinte questionamento: “será que a possibilidade de não se saber a autoria de algo estimula mais práticas ilícitas?”. (PINHEIRO, 2019).

Embora a alternativa é permitir com orientação, vigilância e aplicando medidas disciplinares ou mesmo jurídicas a quem faz uso inadequado, antiético ou mesmo ilegal, surge o dilema de como garantir o conhecimento sobre o que é o certo e o errado se a maioria das pessoas aceitam os Termos de Uso sem ler.

Patricia Peck Pinheiro sobre *Secret*:

> O próprio Secret já está sofrendo as consequências desta atitude nacional da “não informação”, da ignorância às leis, da não leitura do que está nos contratos, de forma intencional, desejada e que leva a uma prática de insegurança jurídica generalizada, pois grande parcela dos descumprimentos às regras acontece pelo mero desconhecimento das mesmas. (PINHEITO, 2019).

A ferramenta *Secret* possui “Termos de Uso”, que exige idade mínima de 13 (treze) anos. O *Secret* também possui política de privacidade, que deixa claro que o anonimato é relativo e que pode informar a identidade do usuário em caso de ordem judicial.

Nesse mesmo sentido:

> Como se não bastasse, o Secret tem, ainda, um Código de Conduta chamado de “Guia da Comunidade”, que proíbe atitudes que sejam ofensivas, agressivas ou discriminatória e fornece um canal de denúncia (legal@secret.ly) para remoção de conteúdos e punição de infratores que podem ser banidos do serviço (perfil bloqueado ou excluído). (PINHEIRO, 2019).

Questiona-se: porque usar um aplicativo como Lulu[2], o *Secret*[3], o Ask.fm[4], todos permitindo declarações anônimas que acabam semeando um ambiente propício para o *cyberbullyng*[5]? Aquele que decide se conectar aceita, mesmo que

[2] Lulu ou Luluvise é uma aplicação multi-plataforma, criado pela Alexandra Chong, que avalia o desempenho dos homens com a extração de informações do Facebook publicando as notas dadas aos internautas (GOMES, 2013).

[3] *Secret* é um aplicativo para Android e iOS que permite postar confissões e compartilhar segredos com amigos anonimamente. Com ele, o usuário também pode ver os que os seus amigos estão postando (BRITO, 2016).

[4] O Ask.fm é uma rede social de perguntas e respostas, que possui aplicativo para *Androit* e iOS. Com ele, o usuário pode questionar seus amigos pelo seu perfil, responder ao que questionam e, também, seguir a todos que achar interessante, para verificar suas respostas periodicamente. (FURTADO, 2014)

[5] Cyberbullying é a violência praticada contra alguém, através da internet ou de outras tecnologias relacionadas ao mundo virtual. Sendo a ação com o objetivo de agredir, perseguir, ridicularizar e/ou assediar. (POLITIZE, 2020)

tacitamente, o resultado da “socialização de dados”, ou melhor, a perda do controle das suas próprias informações. (PINHEIRO, 2016, p. 100).

Sendo assim, muito pior que o anonimato é o efeito da certeza da impunidade no Brasil. Isso sim gera uma crise de autoridade e faz com que jovens que deveriam usar tecnologia para seu autodesenvolvimento intelectual e social acabem distorcendo esta finalidade e geram agressão mútua. (PINHEIRO, 2019).

Todo tipo de liberdade exige educação e um ambiente seguro para se manifestar. Neste sentido, qualquer excesso é prejudicial, seja pela falta da liberdade ou pelo abuso dela. Ainda vamos todos sofrer as consequências dessa nossa delinquência digital. (PINHEIRO, 2019).

Portanto, deve haver uma imposição das autoridades para que toda e qualquer tecnologia permita o atendimento de algumas regras essenciais: o dever de identificação, funcionalidades para o apagamento do conteúdo pelo ofendido, possibilidade de retirada do ambiente visível e exposto, dever de preservação de provas adequadas por parte de fornecedor da solução para viabilizar eventual medida judicial por um prazo mínimo que esteja alinhado com o tempo prescricional. (PINHEIRO, 2016, p. 103).

Verifica-se, portanto, que o veto ao anonimato tem a sua abrangência aos meios de comunicação na Constituição Federal de 1988, no art. 5º, todos têm liberdade de expressão, mas estão sujeitos a responder por suas declarações. Na sequência será abordado o direito à privacidade nos Tratados de Direitos Humanos, fazendo uma investigação histórica até a lei mais recente que protege nossa privacidade.

2.3 O PRINCÍPIO DO DIREITO À PRIVACIDADE NOS TRATADOS DE DIREITOS HUMANOS

A investigação histórica ajuda a confirmar o fato de ser a privacidade um valor desejado hoje, ainda que alguns há pouco tempo, tenham sustentado que em troca dos benefícios proporcionados pela miríade de serviços gratuitos na Internet, as pessoas renunciariam, ou não se importariam, com a violação a esse direito. Além do mais, permite entender as razões históricas da construção normativa, facilitando a compreensão de alguns princípios que foram estampados nas principais legislações sobre o tema ao redor do mundo. (MACIEL, 2019, p.06).

Em 1824, a Constituição do Império reconhecia um certo direito à privacidade, ao proteger o “segredo da carta” e a “inviolabilidade da casa”. A privacidade estava submetida a um conceito mais lastreado na propriedade. Por isso, vê-se apenas referência ao sigilo da correspondência e à inviolabilidade do domicílio. Não há uma proteção da privacidade por si só, pelo seu conteúdo ou por um aspecto mais subjetivo. O que se protegia ali era a invasão, o ato de romper barreiras físicas. (MACIEL, 2019, p.06).

Com a Declaração Universal dos Direitos Humanos, o mundo viu reconhecido um direito de inviolabilidade à vida privada ser alçado a um direito fundamental do homem. O artigo 12 da Declaração estatui que: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques”. (MACIEL, 2019, p.07).

Entrando na década de 1990, começam a surgir, no Brasil, diplomas legais alçando a proteção dos dados pessoais a outro patamar jurídico.

Em 1990, o Código de Defesa do Consumidor (Lei nº 8.078/90), regulou o uso de banco de dados de consumidores. Previu o direito de o consumidor ter acesso a “informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele”, permitindo a correção em caso de inexatidão e, embora não tenha previsto o consentimento para coletar tais dados, exigiu que o consumidor seja informado sobre a abertura do cadastro. (MACIEL, 2019, p.08).

Em 1996 a Lei de Interceptação Telefônica e Telemática (Lei nº 9.296/96) reconheceu o direito à privacidade, ao restringir o uso de tal método investigativo a determinadas hipóteses e sempre sob o amparo de uma ordem judicial. (MACIEL, 2019, p.08).

Em 1997, a Lei do Habeas Data (Lei nº 9.507/97) foi promulgada, regulando o direito constitucional e o rito de acesso e correção de informações pessoais. (MACIEL, 2019, p.08).

Em 2002, o Código Civil Brasileiro trouxe, um capítulo sobre os Direitos da Personalidade, incluindo a vida privada e fornecendo instrumentos para coibir a violação de tal direito. A relevância dessa inclusão, ainda que tardia, revela a privacidade como um direito subjetivo e não focado no direito à propriedade. (MACIEL, 2019, p.08).

No mesmo ano, na União Europeia, foi aprovado o *ePrivacy Directive*, instrumento jurídico equivalente à Diretiva 46, ou seja, sem força obrigatória entre os países membros, porém adotada como norte legal para a implementação de proteção aos dados pessoais coletados e tratados em meio eletrônico. Atualmente a Europa discute a aprovação do Regulamento sobre *ePrivacy*, tornando tais disposições obrigatórias, tal como o GDPR. (MACIEL, 2019, p. 10).

Em 2011, no Brasil, duas importantes legislações foram aprovadas. A Lei do Cadastro Positivo e a Lei de Acesso à Informação.

Foi com o Marco Civil da Internet que o Brasil passou a constar em seu sistema jurídico a palavra “privacidade”. Que abordarei especificamente em outro capítulo.

Em 2014, a Corte Europeia reconheceu aos titulares dos dados o direito ao esquecimento perante os buscadores, como forma de proteção dos dados pessoais (MACIEL, 2019 p. 16).

Maciel, aborda sobre esse direito:

> Esse direito restou garantido no GDPR, porém, na LGDP não foi previsto dispositivo semelhante. Na realidade, entendo que deixar ao critério dos provedores a decisão sobre a retirada ou não de conteúdo é bastante temerário, devendo ser precedido sempre de ordem judicial, 17 porquanto somente o juiz poderá ponderar os direitos em conflito, conforme modelo adotado no Brasil. (MACIEL, 2019 p. 16).

Em 2018 então, o Brasil passou a entrar no rol de países com uma legislação voltada à proteção de dados pessoais, claramente inspirada no regulamento europeu. Com vigência inicialmente prevista para o dia 16 de 18 fevereiro de 2020, com a edição da Medida Provisória nº 869/18, tal prazo foi estendido por seis meses, passando para agosto do mesmo ano.

A vigência da LGPD estava prevista para agosto de 2020, mas algumas tramitações legais acabaram alterando os prazos iniciais. No último mês de agosto, a lei foi aprovada pelo Senado Federal e agora está aguardando a sansão do presidente para que possa entrar em vigor.

Em um capítulo específico da LGPD, estão escritos os direitos do titular, que se baseiam, especialmente, nos direitos fundamentais, pela declaração Universal dos Direitos do Homem, promulgada pela Organização das Nações Unidas. Este capítulo exige que o Controlador e o Operador tenham uma gestão rigorosa de tudo

o que for feito com os dados. Também exige que seja enviada para o titular a qualquer momento que por ele for solicitada uma declaração contendo a discriminação dos dados e de seis tratamentos. (GARCIA et al., 2020, p. 20).

A Lei Geral de Dados Pessoais (LGPD) foi totalmente inspirada no GDPR, sendo este o Regulamento Europeu que dispõe sobre a Proteção de Dados Pessoais e válido para todo o território Europeu. Ao longo dos últimos 30 anos, pode-se afirmar que o Brasil possuiu algumas legislações isoladas que tratavam do tema da privacidade e dos dados pessoais, sempre com o um enfoque secundário, de forma que até então não possuía uma legislação específica sobre o tema e com baixíssimo grau de proteção à privacidade dos dados pessoais, para não dizer nenhuma proteção. (MACIEL, 2019 p. 29).

A sociedade digital já não é uma sociedade de bens. É uma sociedade de serviço em que posse da informação prevalece sobre a posse dos bens em produção. Essa característica faz com que a proteção do Direito a Informação seja um dos princípios basilares do Direito Digital, assim como a proteção de seu contradireito, ou seja, do Direito à não informação. (PINHEIRO, 2016, p. 89).

Verificou-se neste capítulo o direito à privacidade nos Tratados de Direitos Humanos, ficando evidente uma evolução significativa, até a lei mais recente que protege nossa privacidade, totalmente inspirada no regulamento europeu. Na sequência serão analisados a construção da concepção do Direito Digital, suas características, bem como, a evolução da sociedade digital.

3 A CONSTRUÇÃO DA CONCEPÇÃO DO DIREITO DIGITAL

O presente capítulo tem por objetivo apresentar a construção da concepção do Direito Digital, suas características, bem como, a evolução da sociedade digital.

Inicialmente, busca-se esclarecer a conceituação do direito digital, o uso das redes sociais refletida nessa nova sociedade digital e a promulgação da lei chamada Marco Civil da Internet responsável por garantir o direito à informação e a proteção da liberdade de expressão.

3.1 O DIREITO DIGITAL E SUA CONCEITUAÇÃO

Entende-se que o direito é responsável pelo equilíbrio da relação comportamento-poder, que só pode ser feita com a adequada interpretação da realidade social, criando normas que garantam a segurança da expectativa mediante sua eficácia e aceitabilidade, que compreendam e incorporem a mudança por meio de uma estrutura flexível que possa sustentá-la no tempo. Esta transformação leva ao surgimento do Direito Digital. (PINHEIRO, 2016, p. 57)

A informática nasceu da ideia de beneficiar e auxiliar o homem nos trabalhos. Patricia Peck Pinheiro define a informática sendo “uma ciência que estuda o tratamento automático e racional da informação.” (PINHEIRO, 2016, p. 59). O elemento físico que permite o tratamento de dados e o alcance é o computador.

Com as facilidades e trocas de informações, atualizações imediatas e porque não dizer as descobertas e os deslumbramentos, originados com o advento da internet, surgiram diversos crimes e invasões, e também na esteira de quem busca coibi-los, consequentemente surgiram dificuldades inerentes às novas formas utilizadas para a prática dos delitos. Vários fatos contribuíram para uma mudança na realidade social e para um avanço gigantesco do Direito Digital. (MARQUES, 2012).

Reforçando o conceito e evolução do Direito, acrescenta o autor Mario Antônio Lobato de Paiva:

> O Direito Digital ou Direito Informático é o conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador - como meio e como fim - que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do *software*; o comércio eletrônico e as relações humanas estabelecidas via *Internet*. (PAIVA, 2002).

Assim como o Professor Almeida Filho:

> Trata-se do conjunto de normas e conceitos doutrinários destinados ao estudo e normatização de toda e qualquer relação em que a informática seja o fator primário, gerando direitos e deveres secundários. É o estudo abrangente, com o auxílio de todas as normas codificadas de Direito, a regular as relações dos mais diversos meios de comunicação, dentre eles os próprios da informática. (FILHO, 2005).

O direito digital consiste na evolução do próprio direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional, etc.). (PINHEIRO, 2016, p. 77).

Na era digital, o instrumento de poder é a informação, não só recebida, mas refletida. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso a informação. A mudança é constante e os avanços tecnológicos afetam diretamente as relações sociais. Sendo assim o Direito Digital é, necessariamente, pragmático e costumeiro, baseado em estratégia jurídica e dinamismo. O modelo jurídico começa a transformar para viabilizar o exercício de cidadania digital, seja através de ferramentas de peticionamento ou plebiscito online, ou ainda para garantir o direito de estar conectado a Internet como um novo direito essencial do indivíduo. (PINHEIRO, 2016, p. 80).

Sobre as características do Direito Digital, Patricia Peck Pinheiro:

> Celeridade, dinamismo, autorregulamentação, poucas leis, base legal na pratica costumeira, o uso da analogia e solução por arbitragem. Esses elementos o tornam muito semelhante à Lex Mercadoria, uma vez que ela não está especificadamente disposta em um único ordenamento, tem alcance global e se adapta às leis internas de cada país de acordo com as regras gerais que regem as relações comerciais e com os princípios universais do Direito como a boa-fé. (PINHEIRO, 2020, p. 83).

Percebe-se, portanto, que o Direito Digital mostra ser o progresso do próprio Direito, já que não se debate uma nova área, porém e, contudo, todas as áreas já existentes e conhecidas na esfera jurídica que diante dos fatos do seu desenvolvimento passam a integrar questões tecnológicas. Assim, o Direito Digital abrange todos os princípios fundamentais e institutos que estão em vigência e são

aplicados hodiernamente, assim como também introduz novos institutos e elementos para o pensamento jurídico, em todas as suas áreas. (PINHEIRO, 2016, p. 81).

Verificou-se neste capítulo a construção da concepção do Direito Digital, sendo o conjunto de normas e instituições jurídicas que pretendem regular o uso dos sistemas de computador. Na sequência serão analisados sobre o tratamento e cuidados com as redes sociais, tanto pelos usuários físicos e jurídicos.

3.2 AS REDES SOCIAIS E O DIREITO DIGITAL

As redes sociais são consideradas parte da sociedade, sendo elas responsáveis por diversos vínculos, criando novos conceitos de relacionamento social e também da maior liberdade nas mãos de seus usuários, para interagir de modo mais livre e rápido. Ela é utilizada como fonte de pesquisa, entretenimento, notícias, tornando-se interativa e participativa, dando a oportunidade de não só ler o que lhe for cômodo, mas também produzir seu próprio conteúdo. (SILVA et al, 2017).

Nem todas as vezes que as redes sociais foram utilizadas gerou o efeito planejado, virando uma exposição de ódio gratuito, de preconceito e de todas as atrocidades humanas que estão mitigadas e escondidas no contexto social, mas tão expostas nas redes sociais. Levando não somente à brigas, mas também mortes e tudo por um posicionamento diferenciado e extremista. A difamação e calúnia se tornou algo comum e diário, o abuso que foi gerado, a forma em que a falta de respeito e limite, feriram muitos e levou a um extremo, gerando processos criminais, pelo qual essas ofensas começaram a custar caro para aqueles que as fizeram. (SILVA et al, 2017).

Assim, o direito de privacidade se tornou um dos maiores avanços a serem conquistados aos direitos individuais, e um direito que permite ao cidadão o seu espaço privativo. Embasado na privacidade e na constância desse direito, entende-se que a mesma é tudo aquilo que se é preservado, como intimidade e vida privada, para que fique somente ao indivíduo, aquilo que lhe for de vivência. A falta de regulamentação causa uma mácula ao sistema, pois traz consigo um anonimato e de que a falta de legislação do direito de ser feito o que quiser, muitas vezes afetando propositalmente a vida privada de outrem, que ficaria impune. (SILVA et al, 2017).

O sistema judiciário brasileiro já deu alguns posicionamentos sobre o contexto, onde a privacidade foi protegida e foi afixado o dano moral.

> RESPONSABILIDADE CIVIL. DANO MORAL. IMAGEM. PRIVACIDADE. FOTOGRAFIA SEM AUTORIZAÇÃO. INTERNET E JORNAL.
> I - A profissional que atuou como fotógrafa enviada pelo SEBRAE e tirou foto para instruir matéria veiculada por esse no site da internet não tem legitimidade passiva ad causam para compor pólo passivo de demanda na qual se postula indenização por dano moral embasada em uso indevido da imagem. Mantida ilegitimidade passiva da fotógrafa.
> II - A veiculação da fotografia do autor, sem sua autorização, em site da internet e em jornal violou os direitos personalíssimos à imagem e à privacidade, assegurados pela Constituição Federal, art. 5º, inc. X.
> III - A valoração da indenização pelo dano moral, entre outros critérios, deve observar a gravidade, a repercussão, a intensidade e os efeitos da lesão, bem como a finalidade da condenação, de desestímulo à conduta lesiva, tanto para o réu quanto para a sociedade. deve também evitar valor excessivo ou ínfimo, de acordo com o princípio da razoabilidade.
> IV - Apelação provida. (DISTRITO FEDERAL, 2010).

Considerado um fenômeno para a população e muita vez acontece até a associação de internet e rede social no mesmo contexto na concepção de diversos brasileiros as redes sociais vem disseminando uma nova forma de contato, de amizades, negócios e até mesmo relacionamentos diversos, proporcionando aos usuários até casamentos, por outro lado ocorre também diversos tipos de abusos, que já foram inseridos na nossa população. (SILVA et al, 2017).

Os usuários fazem postagens de suas fotos, de seus momentos, expondo suas vidas e relatos importantes, que associam e identificam o seu perfil, não ficando somente preso a ele, mas também a sua família, que fazem parte do que é inserido no mundo virtual, que dá a livre-arbítrio a usuário. (SILVA et al, 2017)

Com isso, no meio de tantas informações e perfis, nasce uma nova incidência de perfis falsos, que são os perfis “fakes”, que tem seu aumento promulgado, pela utilização das imagens de terceiros, podendo atacar a honra e expondo as pessoas ao ridículo, sendo assim, a punição é efetiva, como se encontra na devida legislação brasileira. A utilização dos perfis fakes não é uma forma de crime, mas sim o que o usuário irá fazer com esse perfil, de como ele tira as informações que serão expostas e também de onde essas vieram. (SILVA et al, 2017).

A criação de perfil a partir de uma pessoa viva ou morta e que essa seja real, faz com que o criador possa cometer crime de falsidade ideológica, quando esse causa dano a vítima. Ao se manifestar como outra pessoa, fazer falsos relatos,

afirmar a personalidade via incorporação, fazer declarações, fazer alterações de fatos ou contrarias das que foram versadas no contexto virtual, cria a obrigação de reparação e a feitura de pratica delituosa do agente, e constitui claramente a falsidade ideológica. (SILVA et al, 2017).

O que é notório é que não ocorre muitas vezes a diferenciação de diversão e o abuso, pois nem todo ato será visto como crime, quando só realizado para ocultar e deixar em anonimato tecnológico as suas informações, mas quando são extrapolados alguns limites claros, cometendo diversas condutas delitivas, como os crimes contra honra, calunia, difamação e afins. (SILVA et al, 2017).

A liberdade de expressão, a ausência de censura, o descontrole gerencial do acesso e as diversas informações que são acometidas nesse mundo cibernético, sugere uma falsa impressão ao usuário que todo conteúdo que é armazenado é legalizado, mas quando a atitude do usuário é maligna, será dada a punição, o que muitos não sabem, e utilizam todo e qualquer tipo de informação sem nenhuma precaução, não estando devidamente informados dessa realidade, e não se importando com o que divulgado, até chegar ao ponto de serem solicitados pela Justiça para prestar o esclarecimento de seus atos. (SILVA et al, 2017).

A realização dos crimes que acontecem nas redes sociais se dá pela alusão de que ao estar atrás de uma tela de computador, será auferido anonimato e impunidade, o que é equivoco extremo daqueles que realizam esse tipo de conduta. Tão como a falta de reação de suas vítimas, que estão acostumadas a não reagirem tanto por não saberem como lidar com esse tipo de constrangimento ora por medo de seu possível agressor, quando ocorre o fato por alguém conhecido. (SILVA et al, 2017).

Muitos usuários revelam seus dados pessoais para pessoas que não conhecem, tornando a ação dos infratores muito mais fácil, passando informações como endereço, nome completo, documentação, e diversas informações que podem ser utilizados para causar danos aos que as fornecem. O procedimento a ser realizado é a própria Delegacia Especializada em Crimes virtuais, para que seja registrado um boletim de ocorrência, para a sua devida validação, é necessário o levantamento de provas e que essas sejam levadas no momento da denúncia. O advogado especializado de Direito Digital, após o devido registro, é o modo mais fácil para que seja realizado a justiça e instaurado o devido processo. (SILVA et al, 2017).

Após uma análise dos principais pontos referentes à utilização das redes sociais e sua relação com o Direito, enfatizando as influências que são feitas mediante a utilização das mesmas e a forma com que os usuários expõem seus dados, serão abordados na sequência recomendações para blindagem legal das empresas nas redes sociais.

3.2.1 principais recomendações para blindagem legal das empresas nas redes sociais

Já faz parte da rotina de diversos profissionais usarem sua rede de contatos eletrônicos para buscar respostas e soluções a seus problemas. Também há diversas iniciativas em que a empresa cria um ambiente de colaboração interno ou externo para funcionários envolvendo fornecedores, parceiros e ate clientes, para receber ideias e sugestões. Apesar de atraente, o uso de colaboração em massa e demais formatos de Web 2.0 exigem alguns cuidados jurídicos específicos. (PINHEIRO, 2016, p. 448).

Patricia Peck Pinheiro traz o conceito de web 2.0:

> A web 2.0 é um movimento que indica uma tendência pela quebra de alguns paradigmas, derivado da observação de características comuns aos serviços que estão se consolidando como os mais importantes da Internet. (PINHEIRO, 2016, p. 449).

No entanto, aspectos jurídicos como a questão autoral e trabalhista, devem ser observados. Como a empresa pode se proteger desses riscos jurídicos? Os produtores são, ao mesmo tempo, o público e este também é composto por pessoas que estão apresentando ideia, divulgando ideias e apresentando materiais. Na internet há leis também que serão aplicadas, por isso quem participa dela devem conhecer seus direitos e deveres, de forma a produzir com comprometimento. (PINHEIRO, 2016, p. 449).

É indiscutível que os direitos a expressão e a livre manifestação de pensamento são pilares democráticos e que devem ser defendidos e preservados.

Para tanto, é preciso um termo de uso do ambiente colaborativo, o cadastro é essencial pra se saber a autoria, e incluir declarações como “sua participação é voluntária, não onerosa, de modo algum há geração de qualquer vinculo

empregatício ou remuneratório", deixar claro o que será feito com o conteúdo por ele produzido e inclusive de quem será a responsabilidade. (PINHEIRO, 2016, p. 450).

Embora o uso das redes sociais seja majoritariamente focado no compartilhamento de informações pessoais, os consumidores estão no mundo digital e suas vozes tem ganhado força junto as empresas, que não querem acumular em sua reputação digital. Assim como as pessoas físicas, as marcas também tem direito a preservação de sua reputação, de acordo com entendimentos de juristas de Tribunais Brasileiros. (PINHEIRO, 2016, p. 452).

Até mesmo a Administração Pública observou a necessidade em participar mais de redes sociais para interagir com os cidadãos, mesmo que seus perfis em redes sociais sejam apenas informativos.

Além disso, a empresa deve estar preparada para o fato de que é possível alguém criar um perfil falso no nome da empresa ou de algum executivo da mesma. A empresa deve selecionar bem cuidará e monitorará esse ambiente. Deve ser alguém com legitimidade para falar em nome da empresa como seu porta voz, até porque será sempre bem difícil afastar a responsabilidade da empresa sobre o conteúdo, a não ser na hipótese de ser falso. (PINHEIRO, 2016, p. 454).

Estando ou não a empresa nas redes sociais ela deve preparar-se para as manifestações digitais, que ocorrem independentemente de sua vontade. Logo, monitorar a internet é essencial, é dever do Registro de Incorporação (RI)[6], como do Marketing, do Recursos Humanos (RH), do Serviço de Apoio ao Consumidor (SAC). (PINHEIRO, 2016, p. 455).

Portanto, seguem as principais recomendações para blindagem legal das empresas nas redes sociais:

a) Realizar planejando estratégico (qual o proposito para utilização do canal);
b) Elabore um guia de conduta para seus colaboradores apoiarem de forma segura, ética e legal a presença da sua empresa nesse canal e um Manual de Uso de marca nos canais eletrônicos;
c) Tenha um plano de respostas incidentes definido;
d) Transparência, apresente as informações de maneira mais clara possível;

[6] É o conjunto de atividades, métodos, técnicas e práticas que, direta ou indiretamente, propiciem a interação das áreas de Contabilidade, Planejamento, Comunicação, Marketing e Finanças, com o propósito de estabelecer uma ligação entre a administração da empresa, os acionistas (e seus representantes) e os demais agentes que atuam no mercado de capitais e que integram a comunidade financeira nacional ou internacional. (IBRI, 2020)

e) Cuidado com a publicação de informação confidenciais, divulgação de boatos ou assuntos pessoais nestes canais corporativos;
f) Realizar treinamentos de capacitação;
g) Não deixe de responder as mensagens enviadas;
h) Varie o conteúdo publicado;
i) Monitoramento. Acompanhe o que os usuários estão falando;
j) Utilize as redes sociais de acordo com os Termos e Condições estabelecidas por elas, cada canal possui regras próprias para utilização e constantemente são utilizadas. (PINHEIRO, 2016, p. 456).

O passo mais importante para a proteção da empresa no tocante às redes sociais é a conscientização de suas equipes, não apenas colaboradores, mas inclusive os terceirizado e parceiros, pois basta um comentário para gerar um grande risco reputacional, financeiro e jurídico. Verificar sempre o que estará associado à sua marca, e, sempre que possível, participar na orientação de valores para formação de usuários digitalmente corretos, como sendo um requisito inclusive e responsabilidade social digital. (PINHEIRO, 2016, p. 457).

Após uma análise dos principais pontos referentes à utilização das redes sociais e sua relação com o Direito, verificou-se que as empresas precisam estar preparadas para esse meio digital, sendo o passo mais importante para a proteção da empresa no tocante às redes sociais a conscientização de suas equipes e quanto aos usuários, esses precisam atentar-se com a forma com que expõem seus dados pessoais em aplicativos. Na sequência serão abordados sobre a finalidade da primeira lei criada de forma colaborativa entre sociedade e governo, a Lei do Marco Civil da Internet.

3.3 O MARCO CIVIL DA INTERNET

O Marco Civil da Internet foi inicialmente criado pelo Poder Executivo e é considerada a primeira lei criada de forma colaborativa entre sociedade e governo utilizando-se a internet como meio para o debate.

Devido à importância de se garantir o direito à informação e a proteção da liberdade de expressão, foi promulgada uma lei específica no Brasil para tratar de algumas destas questões chamadas de Marco Civil da Internet. Nos termos do artigo 1º da Lei nº. 12.965/2014:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (BRASIL, 2014).

A internet veio possibilitar não apenas o encurtamento das distâncias com maior eficiência de custos, mas, sobretudo, a multicomunicação, ou seja, transmissão de texto, voz, imagem. A multicomunicação, associada à capacidade de respostas cada vez mais ágeis, permite que a internet se torne o mais novo veículo de comunicação a desafiar e transformar o modo como as pessoas se relacionam na atualidade. (PINHEIRO, 2016, p. 62)

Com essa regulamentação, passou a haver um limite para o uso dos dados de um cliente a partir do momento que se prevê o direito a exclusão da base de dados. Para se evitar que haja uma solicitação que permita o apagamento de provas de autoria, entende-se que deve ser feita a guarda de dados pelo prazo legal que seria de no mínimo 6 meses. (PINHEIRO, 2016, p. 97).

Portanto, a lei delimita o limite, baseando-se na exigência de transparência e aviso prévio do usuário no tocante a que dados são coletados sobre ele e o que é feito com tais informações. (PINHEIRO, 2016, p. 97).

O Marco Civil da Internet impõe uma série de direitos e deveres aos usuários e prestadores de serviço, sendo uma lei, ao mesmo tempo, criticada e aprovada pela sociedade.

Convém destacar também o art. 3º do MCI, que trata dos princípios desta legislação e dentre eles está a 13 proteções dos dados pessoais, na forma da lei.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014).

Patricia Peck Pinheiro sobre o propósito da lei:

> Não podemos esquecer que o proposito inicial do Marco Civil foi o de garantir a privacidade de dados e consumidores e ter a guarda segura dos mesmos (igualando aos demais países do exterior), complementando o texto Constitucional, o Código de defesa do Consumidor e o Código Civil. (PINHEIRO, 2018, p. 99).

A lei exige que toda empresa que colete, armazene ou compartilhe dados de usuários brasileiros tenha que ter uma política de privacidade clara, apresentada previamente para ciência por parte do cliente. Antes dessa lei se um usuário deixasse de ser cliente do serviço seus dados podiam continuar com a empresa, de forma ilimitada, ou seja, para sempre, para uso com qualquer tipo de propósito. (PINHEIRO, 2018, p. 97).

Assim como a Lei Geral de Proteção de Dados Pessoais, o Marco Civil da Internet foi de grande valia para proteção da privacidade e dos dados pessoais que em algum momento tenham trafegado no universo online. Aqui está uma grande diferença entre a LGPD e o MCI, pois este último está vinculado apenas e exclusivamente à utilização da Internet. (SOARES, 2020).

Muito embora já existisse na Europa uma enorme preocupação com a privacidade e proteção de dados pessoais, já existindo, inclusive, diversas Leis e Regulamentos específicos, no ano de 2016 foi promulgado o *General Data Protection Regulation* ou GDPR, que nada mais é que o regulamento Europeu que dispõe sobre a questão da Privacidade e Proteção de Dados Pessoais. Destaca-se que este regulamento se encontra em sua plena vigência desde 25 de maio de 2018, e, sem sombra de dúvidas, foi um dos principais “incentivos” para a promulgação da LGPD no Brasil. (SOARES, 2020).

Portanto, o Marco Civil da internet destacou como premissa principal que deverá ser aplicada a lei brasileira se a atividade foi iniciada, originada ou de alguma forma parcialmente realizada a partir do território brasileiro quando houver algum ato de coleta de armazenamento, de guarda, de tratamento de dados pessoais ou de comunicação ou um dos terminais envolvidos na operação estiver no Brasil (PINHEIRO, 2016, p. 88).

Após análise do Marco Civil da Internet, nota-se que uma das principais intenções do Marco Civil da Internet é a proteção da pessoa natural no mundo

virtual, pois a proteção da dignidade humana deve ser feita em todos os aspectos possíveis da vida social. Existe um crescente uso da internet para comércio e para relações pessoais, nada mais se faz necessário do que uma legislação que proteja a pessoa.

Após esta argumentação sobre a finalidade da primeira lei criada de forma colaborativa entre sociedade e governo, a Lei do Marco Civil da Internet que visa garantir o direito à informação e a proteção da liberdade de expressão. No próximo capítulo será abordado mais uma lei que vem trazendo essa garantia e proteção ao uso de dados pessoais, a LGPD.

4 A LEI GERAL DE PROTEÇÃO DE DADOS

O presente capítulo tem por objetivo apresentar um avanço importante da Lei Geral de Proteção de Dados, frente aos princípios do Direito à privacidade e a vedação do anonimato.

Por fim, abordar pontos de cada um dos capítulos da LGPD, bem como o direito a proteção dos dados pessoais.

4.1 O CUMPRIMENTO DAS NORMAS DA LGPD FRENTE AOS PRÍNCIPIOS DO DIREITO À PRIVACIDADE E A VEDAÇÃO DO ANONIMATO

A LGPD adotou o modelo do regulamento europeu. Embora mais sucinta, seus pilares são praticamente os mesmos. Para tanto, o legislador adotou boa parte do PL 4060/12. (MACIEL, 2019, p. 19).

Sobre a finalidade da lei, Maciel traz que:

> A lei busca um equilíbrio entre os novos modelos de negócio baseados no uso de dados pessoais e a proteção à privacidade, valor cada vez mais na pauta dos cidadãos a partir da divulgação cada vez maior de casos de uso indevido de tais informações. (MACIEL, 2019, p. 19).

A LGPD é um dispositivo que estabelece padrões sobre quais dados de usuários, armazenados por empresas, são pessoais ou sensíveis, além de trazer regras de como eles devem ser tratados e armazenados. A lei dispõe ainda de punições para eventuais descuidos e também fala de uma autoridade nacional para fiscalização. (LAVADO, 2020).

Nesse mesmo sentido, sobre a finalidade da lei, Dino Schwingel:

> Claramente, a lei foi pensada para proteger os cidadãos e consumidores de abusos que possam ser cometidos por grandes organizações e grupos de interesse. No entanto, na sua generalidade, a lei entra em vigor e aplica o mesmo rigor tanto para empresas com faturamento multibilionário quanto para pequenas empresas como clínicas médicas, escolas particulares, entidades assistenciais, filantrópicas e ONGs. (DINO, 2019).

A aplicação da LGPD é basicamente voltada a pessoas físicas e naturais, cujos dados pessoais estejam tendo o tratamento feito por empresas ou órgãos públicos. Veja-se como os objetivos dessa lei ficam claros já no seu artigo 1º:

> 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. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2018).

Nota-se que a intenção do legislador foi deixar claro que esta lei irá regular o tratamento de dados pessoais tanto online, quanto offline, diferentemente do Marco Civil, que regula apenas e exclusivamente os dados pessoais que trafegam na Internet (online). (SOARES, 2020).

A LGPD aplica-se a todas as operações de tratamento realizadas no Brasil, com o objetivo de ofertar bens, serviços ou tratar dados de indivíduos localizados no país ou ainda, que tenham sido coletados no território nacional. (MACIEL, 2019, p. 19).

A proteção de dados pessoais é um tema sensível e de grande relevância para todas as empresas e cidadãos brasileiros, seja em razão de aspectos econômicos, como, por exemplo, o desejo do Brasil em ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), ou seja, em razão de se ter garantido o direito à privacidade e proteção de dados pessoais dos cidadãos, que, desta forma, passam a ter mais confiança sobre a coleta e uso de seus dados pessoais. (SOARES, 2020).

O interesse principal do Brasil ao promulgar a LGPD é o de integrar à Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e para que isto ocorra existe o pré-requisito de uma legislação em plena vigência que trate da Proteção de Dados Pessoais (Lei nº 13.709/18[7]), além do que as referidas diretrizes de proteção de dados pessoais da OCDE deverão ser consideradas como boas práticas para montar e/ou revisar programas de conformidade à LGPD para todas as empresas do Brasil. (SOARES, 2020).

Outro fator de extrema relevância ao Brasil, é quanto ao fato de que a Europa já possui vigorando a sua legislação sobre a proteção de dados pessoais, conhecida como General Data *Protection Regulation* (GDPR), e que, sem sombra de dúvida, impactará nos negócios das organizações Brasileiras, sendo certo que as empresas

[7] A Lei nº 13.709/18 pode ser consultada no site: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 out. 2020.

nacionais que fazem negócios com a Europa precisarão possuir uma política de c*ompliance* de privacidade e proteção de dados para preservar tais relações comerciais. (SOARES, 2020).

O tema de privacidade e proteção aos dados pessoais é um caminho sem volta no mundo, pois conforme amplamente debatido, os dados pessoais estão sendo considerados como o novo petróleo, gerador de riquezas absurdas. Para os agentes de tratamento de dados ficam estabelecidas e pré-definidas as regras do jogo, estando cientes sobre as operações de tratamento de dados (coleta, armazenamento, compartilhamento, etc.), suas possibilidades e impactos, de forma que haverá mais segurança jurídica para os agentes e, em consequência disso, o desenvolvimento econômico e tecnológico estará sendo fomentado. (SOARES, 2020).

Assim, a LGPD não se aplica a dados relacionados às pessoas jurídicas, porquanto já tutelados na esfera da propriedade intelectual. Por outro lado, segundo o seu artigo 4º, a referida lei também não se aplica ao tratamento de dados pessoais realizados por pessoa natural para fins particulares e não econômicos; ou exclusivamente para fins jornalístico, artístico ou acadêmico; bem como para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Além disso, a LGPD também não se aplica a dados de pessoas falecidas e dados em trânsito, ou seja, aqueles que não têm como destino Agentes de Tratamento no Brasil. (BRASIL, 2018).

Em um primeiro momento, a figura anônima ou com a identidade modificada era muito comum, o indivíduo acreditava que podia assumir sua identidade preferida, apresentando-se com um nome, sexo, idade, que poderiam ser diferentes dos dados reais do indivíduo. Com o crescimento da rede esse quadro teve uma mudança significativa, o anonimato passou a ser controlado, a possibilidade de construção de uma nova identidade ainda existe, mas a ideia de uma única pessoa controlar diversas identidades na rede tornou-se um mito, pois, esbarra na questão da liberdade absoluta na rede. A crescente possibilidade do indivíduo se fechar na fortaleza digital oferece apenas um falso sentimento de privacidade. “Mais do que se subtrair do controle social, o indivíduo se encontra na situação de ver rompido o liame social com os seus semelhantes, que se tenta reconstruir com base somente na comunicação eletrônica,” (RODOTÀ, 2008, p. 94) e nessa situação “na aldeia

global aumenta a sensação de auto-suficiência[8], mas também a separação com relação aos demais.” (sic.) (RODOTÀ, 2008, p. 94-95).

O anonimato pode ser usado para violar a privacidade alheia, não pode um indivíduo com identidade diferente da real, difundir na rede notícias difamatórias ou secretas sobre a vida de uma pessoa. Deverá ser feita uma análise de cada caso concreto e uma ponderação entre a privacidade de quem utilizando o manto do anonimato viola a privacidade de alguém, e quem tem sua privacidade violada por uma pessoa que utiliza o anonimato para expor a privacidade alheia. Hoje a tutela da privacidade violada se sobrepõe à privacidade de quem quer anonimato. Por essa razão existem mecanismos eficientes capazes de identificar e localizar o autor do ato ilícito, como o rastreamento do número de IP de cada computador (RODOTÀ, 2008, p. 102).

Ocorre também um controle maior por parte dos provedores de internet, que devem armazenar os dados pessoais e os registros de acesso de cada usuário. O usuário deve revelar esses dados ao provedor, que se compromete a mantê-los em sigilo, só podendo divulgá-lo através de ordem judicial. Dessa forma, equilibra-se o conflito existente entre anonimato e privacidade, colocando limites à liberdade na rede, e responsabilizando os provedores se não tomarem as devidas providências. (RODOTÀ, 2008, p. 103).

No caso de descumprimento da lei, cabe indenização e multa, sendo que o Operador e Controlador são solidários entre si, ou seja, é possível cobrar de um, de outro ou de ambos. Da mesma forma, há possibilidade regresso, ou seja, aquele que pagar a indenização para o titular pode cobrar do outro. Os titulares podem processar de forma coletiva tanto o operador quanto o controlador. (GARCIA et al., 2020, p. 22).

Portanto, fere o direito à privacidade do indivíduo a empresa que recebe os dados pessoais fornecidos por um cliente em uma compra e aliena esses dados para outra empresa de ramo diverso, sem autorização do cliente. A privacidade exige “um tipo de proteção dinâmica que segue o dado em todos os seus movimentos.”. (RODOTÀ, 2008, p. 17).

Cabe por decisão judicial a inversão do ônus da prova. O instituto da inversão do ônus da prova permite que a acusação não apresente provas, mas que o

[8] Ortografia correta: autossuficiência

acusado tenha que apresentar provas de defesa. A LGPD permite que isso aconteça quando entender que a acusação é verossímil e houver hipossuficiência do titular, ou seja, quando uma parte não tem condição econômico-financeira. (GARCIA et al., 2020, p. 22).

A lei também permite o ônus da prova quando a produção de provas para o titular for extremamente onerosa. Os relatórios e evidencias de que o tratamento e arquivamento de dado são realizados de acordo com as orientações da lei se tornam fundamentais em casos processuais, mas também em eventuais fiscalizações da ANPD. (GARCIA et al., 2020, p. 22).

Verificou-se nesse capítulo que a LGPD é um dispositivo que estabelece padrões sobre quais dados de usuários, armazenados por empresas, são pessoais ou sensíveis, além de trazer regras de como eles devem ser tratados e armazenados a lei dispõe ainda de punições para eventuais descuidos e também fala de uma Autoridade Nacional para fiscalização. No próximo item serão abordados sinteticamente os principais aspectos de cada um dos capítulos da LGPD.

4.1.1 Principais aspectos e capítulos da lei geral de proteção de dados

O capítulo I da LGPD trata das disposições gerais da lei. Estão os fundamentos e a apresentação do escopo dela, as definições de cada um dos novos termos e princípios aplicáveis. Sua principal função é nivelar o vocabulário e definir a natureza dos conceitos abordados. (GARCIA et al., 2020, p. 16).

Segundo Garcia et al. (2020), a lei reserva um artigo para excluir itens de seu escopo, deixando claro que não estão sujeitos a ela dados tratados por uma pessoa natural sem qualquer finalidade econômica, aqueles usados para fins artísticos, jornalísticos e acadêmicos. Para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão a infrações penais, haverá legislação específica sobre o assunto e o banco de dados não poderá ser utilizado por empresa privada. Ela também exclui os dados que tenham origem fora do território nacional, desde que não haja compartilhamento, tratamento ou transferência no Brasil.

O primeiro fundamento do capítulo é a privacidade e o segundo é o da autodeterminação informativa, é a garantia de que o titular tenha o direito de decidir

o que será feito com sua informação. Também são fundamentos a liberdade expressão, informação, comunicação e opinião, bem como a inviolabilidade da intimidade, honra e imagem. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade da pessoa humana e o exercício da cidadania, todos previstos constitucionalmente. (GARCIA et al., 2020, p. 17).

Há fundamentos que não são individuais, mas endereçados à sociedade e ao desenvolvimento nacional. São eles: o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor. (GARCIA et al., 2020, p. 17).

A LGPD define como papéis principais:

a) **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
b) **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
c) **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
d) **Encarregado de dados:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação;
e) **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei. (GARCIA et al., 2020, p. 18).

O capítulo II da LGPD dedica-se aos requisitos necessários para o tratamento de dados, especialmente aqueles referentes ao consentimento. Embora seja a mais comum, o consentimento não é a única hipótese em que é possível capturar e tratar os dados. O interesse legítimo também é base legal, se a Organização (ou um terceiro) precisa fazer os tratamentos para oferecer o produto/serviço, ou até mesmo melhorá-los, ou, ainda realizar inovações, estraria coberta por essa hipótese. (GARCIA et al., 2020, p. 20).

Além disso, mesmo que o titular tenha manifestado público seus dados, o controlador e o operador não estão isentos de suas responsabilidades. Os dados sensíveis somente podem ser tratados sem obtenção do consentimento em situações especiais, por exemplo, por órgão de pesquisa e saúde, desde que se responsabilizem pela segurança e não realizam compartilhamento de dados. (GARCIA et al., 2020, p. 20).

O capítulo II finaliza falando sobre o termino do uso de dados, que pode acontecer quando a finalidade do tratamento for alcançada, quando o período previsto para tal tratamento terminar ou por solicitação do titular ou da ANPD. Os dados devem ser eliminados, exceto em caso de obrigação legal de manutenção, de realização de pesquisa, quando for transferido a terceiro ou para uso exclusivo do Controlador. (GARCIA et al., 2020, p. 20).

No capítulo III, estão escritos os direitos do titular, que se baseiam, especialmente, nos direitos fundamentais, inseridos na Declaração Universal dos Direitos do Homem, promulgada pela Organização das Nações Unidas em 1948.

Sobre os direitos dos usuários é importante destacar que:

> Entre os direitos dos usuários estão: confirmação da existência de tratamento consentidos, a revogação de seu consentimento de acesso aos dados, assim como devida correção, anonimização, bloqueio ou eliminação do que não concordar, portabilidade a terceiro que indicar, informações sobre possíveis compartilhamentos. (GARCIA et al., 2020, p. 21).

Este capítulo exige que o controlador e o operador tenham uma gestão rigorosa de tudo o que for feito com os dados. Também exige que seja enviada para o titular a qualquer momento que por ele for solicitada uma declaração contendo a discriminação dos dados e de seis tratamentos. (GARCIA et al., 2020, p. 20).

O capítulo IV é dedicado ao tratamento de dados pelo Poder Público, que pode coletar dados e tratá-los, além das hipóteses do consentimento, nos casos em que houver persecução do interesse publico, para executar suas competências legais ou cumprir com suas atribuições. Caso o Poder Público precise realizar algum ato previsto em lei, poderá coletar os dados necessários, com ou sem consentimento do titular. Isso não exclui os direitos do titular com relação à transparência, ou seja, ele pode solicitar uma declaração de todos os dados aos quais o poder público tem acesso, quais os tratamentos realizados, assim como compartilhamentos, mas não pode solicitar exclusão ou bloqueio se o tratamento estiver previsto nas hipóteses apresentadas. (GARCIA et al., 2020, p. 20).

O capítulo V traz dispositivos sobre a transferência internacional de dados. Destaca-se que a transferência somente pode acontecer para países ou organismos que possuem leis de proteção de dados similares à brasileira. (GARCIA et al., 2020, p. 21).

Nesse sentido apresenta Garcia et al. (2020) que este foi um dos valores da lei nacional:

> Evitar que o Brasil sofresse qualquer embargo comercial por falta de legislação apropriada, especialmente da Europa, após a promulgação por esta da GDPR. Caberá à ANPD definir a lista de países para os quais pode haver transferência de dados. (GARCIA et al., 2020, p. 21).

Um caso em que a transferência é permitida, seriam para a cooperação jurídica entre órgão púbicos, com foco na segurança nacional (inteligência, investigação, persecução); como condição de acordo internacional, ou, ainda, para proteção da vida. Há sempre a possibilidade de o titular dar seu consentimento, permitindo a transferência ou não, no caso da ausência do consentimento a ANPD também será responsável por verificar se nas cláusulas contratuais do titular estão presentes. Já o Poder Público é possível fazer sem o consentimento em casos específicos trazidos pela lei. (GARCIA et al., 2020, p. 22).

O capítulo VI se dedica a descrever os deveres e as responsabilidades do Controlador, Operador e Encarregado. No caso de descumprimento da lei, cabe indenização e multa, sendo que o Operador e Controlador são solidários entre si, ou seja, é possível cobrar de um, de outro ou de ambos. Da mesma forma, há possibilidade regresso, ou seja, aquele que pagar a indenização para o titular pode cobrar do outro. Os titulares podem processar de forma coletiva tanto o operador quanto o controlador. (GARCIA et al., 2020, p. 22).

O capítulo VII se dedica ao tema segurança e boas práticas. Os padrões técnicos mínimos para a proteção dos dados pessoais, inclusive tempo para comunicação e remediação de incidentes, serão definidos pela ANPD. A lei recomenda que a remediação seja feita o mais rápido possível, embora não defina um tempo máximo. (GARCIA et al., 2020, p. 23).

Os capítulos VIII e IX determinam a responsabilidades da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, ou seja, são dois capítulos complementares. O capitulo VIII tem como foco a fiscalização da aplicação da lei, versando especialmente sobre as sanções administrativas a serem aplicadas pela ANPD, além de eventuais sanções civis ou penais. Há também a possibilidade de dar ampla publicidade à infração, e, em todos os casos, é preciso

notificar o motivo do problema e a medidas corretivas planejadas e executadas. (GARCIA et al., 2020, p. 23).

Embora as sanções sigam uma lógica de penalização gradual, o legislador declara de maneira explícita que não necessariamente é preciso seguir alguma gradação. As sanções podem ser aplicadas isolada ou cumulativamente, a depender do caso concreto e seguindo a proporcionalidade. Podem considerar critério objetivos e subjetivos, como gravidade e natureza da infração, boa-fé do infrator, vantagem auferida ou pretendida, condição econômica do infrator, assim como a não adoção de mecanismos de prevenção, existência de políticas de boas praticas e governança e pronta adoção de medidas de correção. (GARCIA et al., 2020, p. 24).

O valor da multa é de 2% (dois por cento) do faturamento da pessoa jurídica em seu ultimo exercício, levando em consideração o faturamento total da empresa ou do conjunto de empresas, por decisão da ANPD, especialmente se houver suspeição de idoneidade (GARCIA et al., 2020, p. 24).

Verificou nesse capítulo que a LGPD é um dispositivo que estabelece padrões sobre quais dados de usuários, armazenados por empresas, são pessoais ou sensíveis, além de trazer regras de como eles devem ser tratados e armazenados a lei dispõe ainda de punições para eventuais descuidos e também fala de uma Autoridade Nacional para fiscalização. No próximo item deste capítulo será abordado o direito à proteção de dados pessoais.

4.2 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados (LGPD) é um avanço importante e nasce da necessidade de regular como as empresas e os órgãos públicos devem tratar os dados pessoais de cidadãos e consumidores na sociedade digital do século XXI, pois cada vez mais a informação é um sinônimo de poder, seja ele político ou financeiro (SCHWINGEL, 2019).

Para a lei, dado pessoal é uma informação relacionada à pessoa natural identificada ou identificável, ou seja, dados como nome, endereço, sexo, Registro Geral (RG), Cadastro de Pessoa Física (CPF). (GARCIA et al., 2020, p. 18).

A lei define dado pessoal sensível como:

> Dado pessoal sensível: é o 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 (art.5º, II). (BRASIL, 2018).

A lei brasileira segue uma tendência internacional, pois após diversos casos de vazamento de dados sensíveis e de abusos por parte de empresas e grupos organizados – cujo ápice pode se argumentar terem sido as tentativas de manipulação nas eleições de 2016 nos Estados Unidos – os legisladores da União Europeia, dos Estados Unidos e de países como o Brasil produziram legislações que visam a resguardar os direitos fundamentais de liberdade, intimidade e de privacidade das pessoas naturais. (SCHWINGEL, 2019).

No contexto atual, verifica-se presente, em relação à proteção de dados pessoais, interesses contrapostos: por um lado, há a proteção da vida privada dos indivíduos e por outro, questões relativas à segurança interna e internacional, reorganização da administração pública e interesses de mercado. (RODOTÀ, 2008, p. 13).

Ainda, o autor defende a proteção coletiva dos dados coletados, mencionando que:

> [...] um alargamento da perspectiva institucional, superando a lógica puramente proprietária e integrando os controles individuais com aqueles coletivos; diferenciando a disciplina de acordo com as funções para as quais são destinadas as informações coletadas; analisando com maior profundidade os interesses envolvidos nas diversas operações e colocando em funcionamento novos critérios para o equilíbrio de tais interesses. Em síntese: a proteção de dados pessoais não pode mais se referir a algum aspecto especial, mesmo que seja em si muito relevante, porém requer que sejam postas em operações estratégias integradas, capazes de regular a circulação de informações em seu conjunto. (RODOTÀ, 2008, p. 50).

O mesmo autor ao analisar demais legislações estipulou outras características necessárias a fim de proteger os dados pessoais, das quais se citam algumas:

> 1. a previsão de colocar à disposição dos usuários não somente instrumentos jurídicos, mas também meios técnicos de controle direto. [...]
> 2. extensão da obrigação de pedir o consentimento dos interessados não apenas para a coleta de dados que lhe digam respeito, mas também para utilização especificas destes [...]. 3. proibição de compartilhar os dados coletados com terceiros [...] (RODOTÀ, 2008, p. 61-62).

A lei também exige o consentimento do responsável legal, quando se trata e dados de menores de 18 (dezoito) anos. Considerando tal público e seu interesse em jogos, a lei endereça um parágrafo para deixar restrita a captura de dados nestes casos, assim como solicita que se trabalhem elementos além de meramente textuais com o intuito de oferecer melhor experiência e entendimento das crianças e adolescentes ao fornecer seus dados (GARCIA et al., 2020, p. 20).

Sem sombra de dúvidas, um dos grandes benefícios decorrentes da promulgação da LGDP é a unificação de todas as regras sobre a questão de privacidade e proteção aos dados pessoais. Antes do início de vigência da LGPD temos uma série de normas que tratavam do assunto de formas isoladas e que não garantiam aos titulares dos dados e aos agentes de tratamento uma segurança jurídica sobre o assunto. (SOARES, 2020).

Acredita-se que os cidadãos também sofrerão os impactos positivos da Lei Geral de Proteção de Dados, pois estes terão resguardados mais uma vez o direito à privacidade e à autodeterminação informativa, que pode ser compreendida como o direito do cidadão em controlar o acesso a seus dados pessoais, diante às inúmeras possibilidades de utilização dos mesmos, principalmente em meios tecnológicos (SOARES, 2020).

Caberá a ANPD a responsabilidade de fiscalizar eventuais abusos ou desvios do Poder Público com relação ao uso de dados, assim cabem a ela eventuais pareceres técnicos sobre dúvidas não endereçadas na lei (GARCIA et al., 2020, p. 20).

A comunicação do incidente deve conter a descrição da natureza dos dados, as informações dos titulares, uma indicação das medidas que foram utilizadas para a proteção de dados, os riscos e os motivos da demora em reverter a situação. (GARCIA et al., 2020, p. 23).

Uma rede de aplicativo anunciou que estava abrindo os seus algoritmos de classificação e compartilhamento, desafiando os seus concorrentes a fazerem o mesmo. A notícia causou impacto entre os desenvolvedores de software, mas deixou perplexa a comunidade técnica, científica e jurídica frente aos reflexos de tal anúncio. Algoritmos são movidos por dados, dados geram informações sobre pessoas, que por sua vez geram mais e mais dados. (FREITAS, 2020).

O tema é tão relevante, que a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), no artigo 20, aponta que:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (BRASIL, 2018).

As técnicas de caracterização de perfil têm como objetivo determinar o que é relevante dentro de um determinado contexto, por exemplo, os interessados em um determinado produto. Estas técnicas auxiliam na representatividade estatística, ou seja, na determinação da qualidade de uma amostra constituída de modo a corresponder à população no seio da qual ela é escolhida. Ou seja, busca-se generalizar a partir de uma amostra de indivíduos e dos seus respectivos interesses. Por exemplo, se um determinado grupo de pessoas está interessado em um determinado produto, outros grupos de pessoas ligados, conhecidos ou relacionados ao primeiro grupo também podem vir a se interessar por este mesmo produto. (FREITAS, 2020).

Pergunta-se, portanto, como explicitar a obscuridade dos algoritmos?

Cinthia Obladen de Almendra Freitas (2020) explica o que é o algoritmo:

> Na Ciência da Computação, um algoritmo é uma sequência finita de ações executáveis que visam obter uma solução para um determinado tipo de problema. Algoritmos devem ser: precisos, não ambíguos, mecânicos, eficientes e corretos. São formados por uma sequência de instruções, raciocínios e/ou operações. Na sociedade contemporânea, tudo se encaixa em algoritmos! Desde relacionamentos (redes sociais, internet banking, telefonia, TV, rádio, música, arte, negócios e vida em tempos de pandemia). (FREITAS, 2020);

É preciso compreender que os algoritmos operam sobre dados e podem: ordenar, classificar, minerar, descobrir conhecimento, agrupar clientes, estabelecer o perfil conhecer gostos e preferências, conhecer qual o comportamento na rede rastrear contatos em tempos de pandemia, indicar produtos, recomendar, reconhecer faces, reconhecer emoções, recuperar informações, tomar decisões: aritméticas, lógicas, relacionais, estatísticas e probabilísticas. Portanto, é importante que os titulares de dados compreendam que os algoritmos mantêm informações longe de nós por meio de bolhas informacionais. (FREITAS, 2020);

O legislador pontuou como importante que os usuários precisam ser informados sobre os algoritmos de tomada de decisão. E, ainda, que caberá “ao

controlador fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial", e no caso do não oferecimento de tais informações, justificado diante de segredo comercial e industrial, "a Autoridade Nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais". (FREITAS, 2020).

A lei coíbe o uso indiscriminado de dados pessoais informados por meio de cadastros e garante ao cidadão o direito de estar ciente sobre como será feito o tratamento de suas informações e para qual finalidade específica elas serão usadas. A lei determina que a empresa deve explicar ao proprietário da informação a razão pela qual vai usar algum dado seu e deve haver um consentimento prévio expresso da pessoa antes da utilização, assim como a transferência de informações para outras empresas. (BRASIL, 2018).

A LGPD, tal qual outros regramentos sobre proteção de dados pessoais, coloca no epicentro do debate a ética dos algoritmos e a formação de uma cultura de dados centrada na proteção de, na segurança da informação, na privacidade e direitos fundamentais.

A lei trouxe regulamentações importantes, como: as entidades devem coletar dados apenas considerados necessários para a realização da tarefa que oferecem ao indivíduo. Dados como orientação sexual, saúde e religião não podem ser usadas com o objetivo de abuso ou discriminação; O usuário que cede seus dados a algum serviço deve ter acesso facilitado ao tratamento deles e à finalidade, bem como saber quem irá manipulá-los.

Portanto, o objetivo maior da lei é preservar a privacidade do indivíduo e seu direito à intimidade, além de mitigar vazamentos sérios de informação.

5 CONCLUSÃO

O presente trabalho trouxe como tema a Lei Geral de Proteção de Dados, Lei nº 13.709/2018, teve como objetivo a verificação dos limites éticos e jurídicos em relação aos usos de informações pessoais dos usuários de serviços digitais por empresas e autoridades públicas para a proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais.

A inviolabilidade do direito à privacidade vem ganhando força nas redes sociais, necessitando-se de leis e punições severas aos que afrontam as normas constitucionais. O direito à privacidade é devidamente assegurado como direito personalíssimo por se tratar de atos da vida pessoal, abarcando as pessoas físicas como as jurídicas, isso implica dizer que a própria pessoa tem a capacidade de domínio da sua imagem e da sua reputação da mesma maneira que poderá ou não disponibilizar as informações a seu respeito.

Os cidadãos têm o direito à privacidade de suas informações mais íntimas e de saber como seus dados são utilizados. Ele tem o direito de saber qual a finalidade específica do tratamento, qual a forma e duração, quem e qual o contato do controlador, se há uso compartilhado e quais as responsabilidades dos agentes que realizam o tratamento. Portanto cabe a cada empresa disponibilizar em site ou aplicativos Termos de Política de privacidade. A principal importância desta política liga-se à transparência e à credibilidade, a política de privacidade deve ser clara e visível. Os usuários devem saber como seus dados serão utilizados para autorizar ou não sua captação.

Sem regras, os internautas estariam sujeitos a violações da privacidade, da intimidade, da livre iniciativa e livre desenvolvimento da personalidade, entre outras consequências como o anonimato, um obstáculo à segurança no ambiente virtual por conta da probabilidade do agente adentrar-se secretamente para o cometimento do ato ilícito e isso o torna distintamente oposto ao sentido do Direito à Privacidade, sendo vedado pela CF.

LGPD é a Lei Geral de Proteção de Dados, uma lei aprovada em agosto de 2018 no Brasil, entra em vigor a partir de 1º de agosto de 2021, lei essa que foi fortemente inspirada pelo GDPR, que é o Regulamento Geral Europeu sobre Proteção de Dados. Ela traz regras sobre o tratamento de dados pessoais,

transparência e que tem como finalidade proteger o direito à liberdade, privacidade e livre desenvolvimento dos cidadãos. Prevê que empresas e órgãos públicos devem mudar a maneira como coletam, armazenam, usam e compartilham dados pessoais.

Diante de tal, admite-se a importância da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. As penalidades vão desde advertências até o bloqueio dos dados. Para a definição da sanção, serão analisados critérios como a gravidade da infração, a boa-fé do infrator, possível reincidência e outros elementos listados na lei. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Observou-se também que o Marco Civil é uma espécie de “Constituição da Internet”, visando à regulamentação, dos direitos e deveres dos usuários da internet, dos portais e sites, das prestadoras de serviço e do Estado. Trata-se, portanto, de uma institucionalização burocrática sobre o que é certo e o que é errado no mundo virtual. Responsável por garantir o direito à privacidade e a liberdade dos usuários que utilizam a internet.

O processo de desenvolvimento tecnológico é um caminho sem volta isso é fato inconteste. Ao Direito e aos seus operadores compete amoldarem-se a esta nova configuração, propondo discussões para deliberarem acerca das justas, eficazes e céleres resoluções, seja na informatização processual seja para dirimir os conflitos presenciais ou virtuais a fim de acompanhar uma sociedade cada vez mais digital.

Constatou-se que, a LGPD cumpre, então, o seu papel de proteção de dados, pois assegura aos titulares a forma mais justa e moderna de responsabilização civil que há no nosso ordenamento jurídico. A Lei Geral de Proteção de Dados, ao fazer uso de seus aspectos para o tratamento dos dados, é satisfatória ao ponto que é eficiente em atender as mais diversas demandas relacionadas a proteção de dados pessoais. Institui um sistema de transparência, objetividade e segurança que assegura a identificação de falhas e possibilidade o restabelecimento de seus efeitos. Implementa um sistema de reparação que distingue bem as relações que se aplicam a responsabilidade civil subjetiva e objetiva, de modo a efetivar a reparação do titular, preservando os fundamentos constitucionais. Dessa forma, se diz que os objetivos deste trabalho puderam ser contemplados.

REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo. **Direito Eletrônico ou Direito da Informática?** Informática Pública vol. 7 (2): 11-18, 2005. Disponível em: http://www.ip.pbh.gov.br/ANO7_N2_PDF/IP7N2_almeida.pdf. Acesso em: 10 mar. 2020.

BRASIL, Constituição (1998). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1998. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 26 mar. 2020.

BRASIL. **Lei 13.105, de 16 de março de 2015**. Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 14 out. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 abr. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 05 fev. 2020.

BRITO, Edivaldo. **Use o app Secret para descobrir todos os segredos de seus amigos.** G1. Tecnologia e Games. 16/11/2016. Disponível em: https://www.techtudo.com.br/tudo-sobre/secret.html#:~:text=Secret%20%C3%A9%20um%20aplicativo%20para,os%20seus%20amigos%20est%C3%A3o%20postando.&text=Ap%C3%B3s%20muitas%20pol%C3%AAmicas%2C%20o%20Secret%20foi%20retirado%20da%20App%20Store%20brasileira. Acesso em: 14 out. 2020.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios. **Apelação nº 20789320088070008/DF**, 0002078-93.2008.807.0008, Relator: Vera Andrighi, Data de Julgamento: 03 de fevereiro de 2010, 1ª Turma Cível, Data de Publicação: 08 de março de 2010, DJ-e pág. 143. Disponível em: https://tj-df.jusbrasil.com.br/jurisprudencia/8179588/apelacao-ci-vel-apl-20789320088070008-df-0002078-9320088070008. Acesso em: 14 out. 2020.

FREITAS, Cinthia Obladen de Almendra. **A obscuridade dos algoritmos e a LGPD. 2020.** Disponível em: file:///C:/Users/Biblio/Downloads/A%20obscuridade%20dos%20algoritimos%20e%20a%20LGPD%20(1).pdf. Acesso em: 15 set. 2020.

FURTADO, Teresa. **Baixe Ask.fm e tenha a rede social de perguntas e respostas no celular**. Techtudo. Downloads. 21/03/2014. Disponível em: https://www.techtudo.com.br/tudo-sobre/ask-fm.html. Acesso em: 14 out. 2020.

GARCIA, Lara Rocha et al. **Lei Geral de proteção de dados (LGPD): Guia de implementação.** São Paulo: Blucher, 2020.

GOMES, Helton Simões. **App para mulher avaliar rapazes, Lulu vira hit e já é usado como vingança**. G1. Tecnologia e Games. 23/11/2013. Disponível em: http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2013/11/app-para-mulher-avaliar-rapazes-lulu-vira-hit-e-ja-e-usado-como-vinganca.html. Acesso em: 14 out. 2020.

IBRI. Instituto Brasileiro de Relações com Investidores. **O que é RI**. Disponível em: http://www.ibri.com.br/educacao-e-pesquisas/o-que-e-ri. Acesso em: 14 out. 2020.

LAVADO, Thiago. **Medida Provisória adia Lei Geral de Proteção de Dados para 2021**. Abril, 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/04/29/medida-provisoria-adia-lei-geral-de-protecao-de-dados-para-2021.ghtml. Acesso em: 30 abr. 2020.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** RM Digital Education. 1ª Edição. Goiânia – GO. 2019.

MARQUES, Jader; Silva, Mauricio Faria da. **O direito na era digital.** Porto Alegre: Livraria do Advogado Editora, 2012.

PAIVA, Mário Antônio Lobato de. **Os institutos do direito informático.** Maio, 2002. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/30390-31543-1-PB.pdf . Acesso em: 23 abr. 2020.

PINHEIRO, Patricia Peck. **Direito digital**. 2ª ed. revista, atualizada e ampliada. São Paulo: Saraiva, 2016.

PINHEIRO, Patricia Peck. **#Direito digital**. 6ª ed. São Paulo: Saraiva, 2019.

POLITIZE. **Cyberbullying**: O que é? Disponível em: https://www.politize.com.br/cyberbullying-o-que-e/#:~:text=Cyberbullying%20%C3%A9%20a%20viol%C3%AAncia%20praticada,%2C%20ridicularizar%20e%2Fou%20assediar. Acesso em: 14 out. 2020.

RODOTÀ, Stefano**. A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SILVA, Karlysson Carvalho et al**. As influências das redes sociais no Direito. Abril, 2017.** Disponível em: https://jus.com.br/artigos/56649/as-influencias-das-redes-sociais-no-direito. Acesso em: 07 out. 2020.

SCHWINGEL, Dino. **A Lei Geral de Proteção de Dados deve ser igual para todos?.** Março, 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/a-lei-geral-de-protecao-de-dados-deve-ser-igual-para-todos/. Acesso em: 30 abr. 2020.

SOARES, Felipe. EBOOK- **Lei Geral de proteção de dados: da privacidade no Brasil às penalidades de descumprimento da lei.** 2020. Disponível em: file:///C:/Users/Biblio/Downloads/E-book%20%20Lei%20Geral%20de%20Proteção%20de%20Dados%20Pessoais%20(LGPD).pdf. Acesso em: 09 set. 2020.