PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

A FUNCIONALIDADE DO DIREITO DIGITAL COM A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

ORIENTANDO: MURILO LOPES SILVA

ORIENTADOR: PROF. JOSÉ EDUARDO BARBIERI

GOIÂNIA-GO
2023

MURILO LOPES SILVA

A FUNCIONALIDADE DO DIREITO DIGITAL COM A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Orientador: Prof José Eduardo Barbieri

GOIÂNIA-GO
2023

MURILO LOPES SILVA

A FUNCIONALIDADE DO DIREITO DIGITAL COM A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

Data da Defesa:_____de_____de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. José Eduardo Barbieri Nota

_____

Examinador Convidado: Prof. Dr. José Humberto Abrão Meireles Nota

Dedico este trabalho aos meus pais, que sempre me motivaram e apoiaram ao longo desses cinco anos de desafios acadêmicos, e também à minha irmã, que esteve ao meu lado durante todo o curso. Sou grato por todo o suporte que recebi deles, e jamais me esquecerei dessa experiência na universidade.

AGRADECIMENTOS

Agradeço a Deus, em primeiro lugar, por todas as bênçãos e oportunidades que ele tem me concedido ao longo da minha jornada acadêmica. Sua orientação divina e amor incondicional têm sido fundamentais para o meu crescimento e sucesso. Sou grato por sua presença constante em minha vida, guiando-me em cada passo do caminho e dando-me força nas horas de dificuldade.

Agradeço imensamente ao meu orientador, Professor José Eduardo Barbieri, por sua valiosa ajuda e orientação durante todo o processo de elaboração e desenvolvimento do meu trabalho. Sua dedicação e expertise foram fundamentais para o sucesso desse projeto

Também quero expressar minha gratidão ao Professor José Humberto Abrão Meireles, sua presença e conhecimentos abrangentes foram de extrema importância para o meu desenvolvimento acadêmico. Além disso, sou grato por sua sabedoria em lidar com as adversidades da vida, ensinando-me a viver com alegria e resiliência. Sou verdadeiramente privilegiado por tê-lo como professor e examinador e exemplo em minha jornada acadêmica.

Além disso, quero agradecer por sua energia positiva e entusiasmo contagiante. Sua presença em sala de aula sempre trouxe inspiração e motivação para mim e para meus colegas. Com otimismo e determinação, por seu apoio constante e ajuda inestimável durante toda a minha trajetória na faculdade. Sua dedicação em compartilhar conhecimentos e sua habilidade em abordar uma variedade de temas foi fundamental para que eu concluísse meu curso com êxito. Sou profundamente grato por todo o suporte que recebi de você ao longo desses anos.

Gostaria de expressar minha gratidão a três pessoas muito especiais em minha vida: meu pai, minha mãe e minha irmã. Sem o apoio e o amor incondicional deles, eu não teria chegado tão longe. Eles estiveram ao meu lado em todos os momentos, me incentivando, me ajudando e me dando forças para continuar.

Meu pai sempre foi um exemplo de determinação e trabalho duro. Ele me ensinou a importância de perseverar, de nunca desistir dos meus sonhos e de sempre buscar o melhor em tudo o que faço. Sua presença em minha vida é uma bênção que eu nunca vou esquecer.

Minha mãe sempre foi minha fonte de amor e conforto. Ela me apoiou incondicionalmente em todas as minhas decisões e me ensinou a importância da empatia, da gentileza e da compaixão. Eu não poderia ter pedido uma mãe melhor.

Minha irmã esteve comigo durante cinco anos do meu curso de direito. Nós estudamos juntos, compartilhamos desafios e vitórias e crescemos juntos como pessoas e profissionais. Sua presença foi essencial em minha jornada acadêmica, e eu sou grato por ter ela como minha irmã.

A todos eles, eu digo: muito obrigado. O amor e o apoio de vocês são a minha maior inspiração. Eu não poderia ter chegado até aqui sem vocês. Vocês são minha família e meu porto seguro. Eu amo vocês.

RESUMO

O tema escolhido tem como objetivo auxiliar aqueles que possuem menor conhecimento a respeito de seus dados deixados em sites, blogs, ecommerce, e outros meios de capitação de dados pessoais. Será apresentado as leis que protegem os usuários da internet, faremos uma abordagem ao risco da exposição de dados e suas consequências. No decorrer será abordado a implementação da lei geral de proteção de dados pessoais, sendo essa, LGPD, criada no Brasil. Compreendendo que essa lei é um avanço para a proteção da pessoa usuária das plataformas digitais, diminuindo o risco e dificultando o acesso para cibe criminosos na utilização e compra desses dados deixados todos os dias pelas pessoas, assim como o avanço da tecnologia com a utilização de robôs e inteligência artificiais as leis também estão avançando para proteger seus usuários. No decorrer deste Artigo, tudo foi realizado visando compreender qual a essência da lei geral de proteção de dados pessoais, isto é, da LGPD que se aplica no Brasil. Considerando as particularidades deste instrumento, observa-se que o seu uso implica em uma valiosa conquista para a proteção da pessoa, mediante o salvaguardar dos seus dados pessoais em bancos de dados informacionais de todos os tipos e tamanhos. Sendo assim, de forma paulatina aqui também, esboçaram-se alguns aspectos, bem como, as prováveis vinculações que se observam entre a proteção da individualidade da pessoa com combate aos crimes digitais pela proteção de dados presentes em bancos de dados informacionais pelo uso da LGPD. Agindo desta maneira, foi possível entender, por qual razão muitas críticas estão sendo apresentadas quanto à utilidade deste instrumento normativo no âmbito da manutenção da ordem e da paz pública no espaço Digital. Pela perspectiva metodológica, este artigo se efetiva mediante uma revisão bibliográfica que se fundamenta na abordagem qualitativa. A sua principal fonte de pesquisa são artigos dissertações teses e livros que se dedicam ao estudo do direito digital no Brasil.

Palavras-chave: Crimes Ciberneticos. LGPD. Dados Pessoais. Direito Digital. Ecommerce.

ABSTRACT

The chosen topic aims to assist those who have less knowledge about their data left on websites, blogs, ecommerce, and other means of personal data collection. The laws that protect internet users will be presented, and the risks of data exposure and its consequences will be addressed. Throughout the article, the implementation of the General Data Protection Law, or LGPD, created in Brazil, will be discussed. Understanding that this law is a step forward in protecting users of digital platforms, reducing the risk and making it more difficult for cybercriminals to access and purchase data left by people every day, as well as the advancement of technology with the use of robots and artificial intelligence, laws are also advancing to protect users.

Throughout this article, everything has been done to understand the essence of the General Data Protection Law, that is, the LGPD that applies in Brazil. Considering the particularities of this instrument, it is observed that its use implies a valuable achievement for the protection of individuals, by safeguarding their personal data in information databases of all types and sizes. Thus, gradually, some aspects were outlined, as well as the probable links that are observed between the protection of the individuality of the person with the fight against digital crimes by protecting data present in information databases through the use of the LGPD. By acting in this way, it was

possible to understand why many criticisms are being presented regarding the usefulness of this normative instrument in the maintenance of order and public peace in the digital space. From a methodological perspective, this article is carried out through a bibliographic review that is based on a qualitative approach. Its main source of research is articles, dissertations, theses, and books that are dedicated to the study of digital law in Brazil.

Keywords: Cybercrimes. LGPD. Personal Data. Digital Law. Ecommerce.

SUMÁRIO

INTRODUÇÃO

A lei se fez necessária para a proteção dos dados pessoais e para a diminuição de crimes cibernéticos, a Lei Geral de Proteção de Dados é resultado de um movimento espontâneo da sociedade e autoridades brasileiras. Desde o início da década, empresas e usuários vêm buscando respostas para as questões de segurança virtual, que ganham relevância em função da escalada do cibercrime. Em 2018, segundo um estudo da McAfee, o Brasil registrou perdas progressivas com crimes virtuais, chegando a R$ 10 bilhões por ano.

A Lei Geral de Proteção de Dados é um conjunto de novos conceitos jurídicos, dados pessoais e dados sensíveis, foi estabelecido condições importantes de direitos para os titulares dos dados, gerando assim obrigações específicas para o controle dos dados e cria uma série de procedimentos e normas para que haja um maior cuidado com o tratamento de dados pessoais e compartilhamento com terceiros. Aplicando assim a toda informação relacionada com a pessoa natural identificada ou que possa ser identificável e aos dados que tratem de origem racial ou étnica, convicção religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, sempre que eles estiverem vinculados a uma pessoa natural

Agora as empresas são responsáveis por aplicar mais segurança e promover políticas de transparentes sobre o uso, isso se deve ao fato de que as pessoas passaram a ter mais autonomia de seus dados. O DPO (Data Protection Officer), ou encarregado de dados, é o profissional responsável por avaliar, opinar, educar e monitorar o tratamento de dados pessoais em uma organização.

Esse profissional auxilia a empresa no cumprimento das obrigações previstas na LGPD. Entretanto, em caso de descumprimento da lei, a responsabilidade será da organização, não do DPO.

Após mudança na LGPD, o DPO passou a poder ser tanto pessoa física como jurídica, interna ou externa da organização (DPO as service). Ao contrário da GDPR, a LGPD não exige que o DPO comprove que tenha conhecimento jurídico ou regulatório sobre proteção de dados. Porém, tal como na prática internacional, algumas habilidades são altamente recomendáveis: Conhecimentos de proteção de dados e segurança da informação adequados às realidades da organização;

Capacidade para garantir a adequada comunicação e troca de informações entre titulares, organização e ANPD; Conhecimentos jurídicos e regulatórios especializados; Capacidade de trabalho interdisciplinar com equipes de TI, legal e

negócios. Embora não haja exigência expressa neste sentido, recomenda-se que a atividade seja desenvolvida por pessoa com autonomia, à semelhança de figuras como o compliance officer e o ombudsman, mas que conheça o negócio e os procedimentos de tratamento de dados pessoais da empresa.

O ciberataque é um assunto delicado e muito se falado atualmente, foi assunto do momento no mercado financeiro empresarial. O tema ganha notória repercussão, que passa a punir administrativamente as empresas que não estão enquadradas aos aspectos dos artigos 52,53 e 54 da lei.

Um dos motivos mais preocupantes, conforme aponta o relatório global ‘Tendências de Ataques Cibernéticos: Relatório do Primeiro Semestre de 2021’, da Check Point Research, que revela como os criminosos cibernéticos continuaram a explorar a pandemia de Covid -19 e destaca um aumento global dramático de 93% no número de ataques de ransomware. De acordo com o relatório com a manutenção do trabalho remoto, ou o modelo híbrido em 2021, os cibercriminosos continuaram a adaptar suas práticas de trabalho a fim de explorar essa mudança, visando as cadeias de suprimentos das organizações e os links de rede para parceiros a fim de obter o máximo de interrupção.

Os números globais dão conta de um aumento de 29% no número de ataques as empresas no primeiro semestre. Apenas na região das Américas foi registrado um aumento de 34% de ataques no período. De acordo com o relatório os tipos ataques maliciosos mais comuns que aparecem nas Américas são Botnet (22%), Banking (14%), Criptomineração (12%), InfoStealer (11%) e Mobile (10%).

O relatório também destaca o aumento dos ataques de ransomware com extorsão tripla, que inclui o sequestro dos dados com a ameaça de divulgação se não houver o pagamento do resgate não apenas da empresa, mas de toda a sua cadeia de fornecedores. "Percebe-se que os invasores agora estão visando os clientes e parceiros de negócios das organizações e exigindo resgates deles também", diz a texto da pesquisa. Por fim, as previsões da empresa para o segundo semestre de 2021 dizem que os criminosos seguem se aperfeiçoando e devem avançar nas práticas dos crimes virtuais. "O ransomware crescerá apesar da intensificação da aplicação da lei. Os crackers estão usando ferramentas de penetração para dar a eles a capacidade de personalizar os ataques em tempo real. Esta tendência crescente está infligindo danos colaterais à vítima-alvo inicial, exigindo uma estratégia de danos colaterais". Alguns usuários que já foram hackeados alegam prejuízos materiais e emocionais, por ser um ataque muito grosseiro, são feitos empréstimos em nomes de terceiros e exposição de fotos das vítimas entre inúmeras formas para subtrair dinheiro

dessas vítimas, a forma como qual eles preferem receber o dinheiro é via criptomoedas principalmente aquelas que não podem ser rastreadas e localizados os proprietários.

Em um mundo cada vez mais digital e conectado, a proteção dos dados pessoais e a privacidade online são temas fundamentais para a garantia dos direitos dos cidadãos e para o desenvolvimento da sociedade. A LGPD e o Marco Civil da Internet são importantes avanços na regulamentação e proteção dos dados pessoais e da privacidade online no Brasil, mas ainda é preciso avançar em relação à conscientização e cultura de proteção dos dados pessoais e da privacidade online.

1 A Funcionalidade do Direito Digital Com a Implementação da Lei Geral de Proteção de Dados

1.1 O Tratamento dos Dados Pessoais

De acordo com Danilo Doneda (2010), a segurança de dados pessoais, tem como finalidade a proteção do titular e, portanto, cria um regime de obrigações para a realização do tratamento destes dados. Nos dias atuais, a proteção de dados vem sendo considerada por inúmeros juristas um Direito fundamental e, desta forma, um meio de concretização das liberdades individuais no mundo virtual. Portanto devemos proteger o bem primordial que é a segurança individual dos dados pessoais, assim evitando riscos de invasões indevidas tanto no meio digital, plataformas de redes sociais e também possíveis fraudes no sistema bancário atual.

Ainda conforme Danilo Doneda (2010), a determinação da ideia da proteção de dados surge para regulamentar a utilização das informações pessoais, dentre as variadas operações às quais ela pode ser submetida, logo após ter sido colhida por um algoritmo.

O tratamento dos dados deve obedecer, entre outros princípios, aos princípios da finalidade, para a minimização da coleta e retenção mínima. Os dados devem ser utilizados apenas para as finalidades especificas para as quais foram coletados e devidamente informadas aos titulares, pelo princípio da minimização da coleta, somente devem ser coletados os dados mínimos necessários para que se possa atingir a finalidade. (ALAN MOREIRA LOPES, DIREITO DIGITAL E LGPD NA PRÁTICA, 2023, p. 48).

Igor Bonfim Viana (2018) destaca em uma análise sistemática da Lei nº 13709/18, que não há proteção aos dados anônimos, afinal como se extrai dos Artigos 1º e 5º, os dados pessoais pressupõem a identificação ou possibilidade de identificação do titular. Deste modo, a LGPD, como também é conhecida, prevê que dados anônimos não podem ser considerados pessoais, apenas quando for possível a reversão da condição anônima.

Consequentemente, a norma em questão cuida em tratar de forma diferente os vários tipos de dados, diferenciando o tratamento de dados pessoais comuns, de dados pessoais sensíveis e dados de crianças e adolescentes, aplicando aos dois últimos, regras mais rígidas (VIANA, 2018).

No tema legal da referida Lei, o Artigo 7º, elenca todas as hipóteses de tratamento das informações pessoais gerais, visto que a primeira se dá a partir do consentimento do titular, devendo ser livre, inequívoco, formado pelo conhecimento das informações necessárias para a tomada de decisão e restrito a finalidade informada ao titular dos dados (BRASIL, 2018). Sendo assim com o avanço da tecnologia são criados algoritmos e robôs capazes de capitar e armazenar os dados em um grande servidor, e, portanto, nesses servidores tem um espaçamento para cada usuário e as empresas são capazes de identificar o comportamento de cada usuário pelas coletas de dados feito durante o uso das plataformas digitais e pela forma como a pessoa busca determinado assunto ou produto. As plataformas digitais possui um mecanismo que armazena a quantidade tempo que a pessoa fica em determinado local como (site, ecommerce, rede social), praticamente elas detém um conhecimento muito grande sobre seus usuários e vendem esses dados para outras empresas, para o fornecimento de novos marketing e produtos para determinado grupo de pessoas, devemos observar que os dados estão sendo coletados sem o consentimento dos usuários do meio digital, não deixando claro qual é o objetivo da coleta dos dados e qual a sua funcionalidade dentro dos aplicativos e sites e o mais prejudicial quando há a informação de coleta de dados conhecido como termos e condições apenas possui um único botão que seria aceitar todos os termos, sem a possibilidade do usuário bloquear e não permitir a sua coleta de dados sendo assim invasivo ao usuário e sendo ilícito a sua coleta

Por outro lado, o Artigo 8º aponta que não é permitida, em hipótese alguma, a extração da omissão do titular dos dados. Por fim, a norma disciplinada diz que o consentimento poderá ser revogado a qualquer instante por um procedimento gratuito e facilitado e qualquer alteração no modo de processamento de dados exigirá novo consentimento, conforme disposto no Artigo 8º, § 5º (BRASIL, 2018).

Outra hipótese disposta está no Artigo 7º, para tratamento de dados pessoais é em caso de cumprimento de obrigação legal ou regulatória pelo controlador. Nesta situação, sobressai-se o interesse público em face do interesse privado do titular, entretanto, tal situação não exclui os direitos do usuário, devendo o controlador observar os princípios da limitação da finalidade do tratamento uso dos meios adequados, informação do titular quanto ao processamento dos dados e, posteriormente a disponibilização dos dados nos termos exigidos pela autoridade nacional (BRASIL, 2018).

Ainda presente no Artigo 7º, o inciso VI possibilita o tratamento de dados para um exercício regular de direitos no processo judicial, administrativo ou arbitral, permitindo o uso de dados pessoais como prova documental em litígio. Em seguida, os incisos VII e VIII preveem o uso de dados pessoais para a proteção da vida, integridade física e saúde do titular e de terceiros, tratamento para tutela de saúde em procedimentos realizados por profissionais da saúde, hipóteses estas que novamente colocam o interesse público sobre os interesses do titular (VIANA, 2018).

Posteriormente, a última hipótese que admite o tratamento dos dados pessoais é a proteção de crédito. Este dispositivo trata da peculiaridade da proteção do crédito, devendo observar a legislação pertinente à temática.

Diante deste contexto, Igor Bonfim Viana (2018) enfatiza que as hipóteses de tratamento de dados sensíveis, são em sua maioria, as mesmas dos dados pessoais, exceto nos casos de execução de contratos, proteção do crédito e do legitimo interesse do controlador.

No que diz respeito ao processamento de dados pessoais de crianças e adolescentes, a norma trata de forma igual aos dados sensíveis ou comuns. O tratamento dos dados de crianças e adolescentes deve visar o melhor interesse do titular, nos termos do Artigo 14, podendo ser realizado em caso de consentimento de pais ou pelo responsável legal (BRASIL, 2018).

É válido ressaltar que a referida Lei Geral de Proteção de dados teve sua *Vacatio legis* alterada pela medida provisória 959, de 29 de abril de 2020. Fazendo

valer a eficácia da Lei a partir de 03 de maio de 2021. Entretanto, estão vigentes desde 28 de dezembro de 2018, após as devidas mudanças acometidas pelos vetos presidenciais, e posterior análise destes vetos pelo congresso, os artigos 55 e 58, que regulam a criação da Autoridade Nacional de Proteção de Dados, também conhecida por ANPD, que será discutida em outro tópico deste trabalho.

Por fim, absorvido o tópico, nota-se que o tratamento de dados pessoais está diretamente ligado à proteção do consumidor. Visto que é de suma importância que as proteções legais vigentes atinjam o consumidor brasileiro.

1.1.1 Políticas públicas

De acordo com, Brasil (2018), em 14 de agosto de 2018, sancionou-se a Lei 13709, a Lei Geral de Proteção de Dados Pessoais (LGPD), diploma nacional voltado exclusivamente para regulação da garantia de guarda das informações pessoais. A Lei se estabelece pelos fundamentos já mencionados anteriormente, seguindo os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, de acordo com o Artigo 6º e seus incisos.

A referida Lei traz disposições sobre a temática e altera dispositivos do Marco Civil da Internet. A Lei não trata especificamente da segurança dos dados pessoais na rede, porém se apresenta como um avanço significativo para a garantia da privacidade no mundo digital (FORTES, 2016; BRASIL, 2018).

Nesta perspectiva, o ordenamento jurídico brasileiro já havia sancionado três legislações que passaram a considerar o mundo virtual como um espaço que exige uma regulação adequada, através da edição da Lei de Acesso à Informação, de 2011; da Lei de Crimes Informáticos, em 2012 e do Marco Civil da Internet em 2014 (FORTES, 2016).

Ainda de acordo com Vinicius Borges Fortes (2016), a Lei nº 12527/2011 foi a primeira norma jurídica contemporânea recepcionada no contexto da Internet, visando garantir o direito fundamental de acesso à informação, aliado a princípios da

administração pública, como observância de uma publicidade para a divulgação de informações de interesse público por meio de métodos proporcionados pela internet, dentre outros.

No tema legal, a Lei nº 12527/11 obriga os entes subordinados a ela a tratarem os dados pessoais de modo transparente, respeitando os direitos fundamentais de intimidade, privacidade, honra e imagem dos indivíduos. Deste mesmo modo, limita o controle de informações, dando um prazo máximo de 100 (cem) anos para acesso aos dados, também como possibilita o acesso a divulgação de terceiros apenas em caso de consentimento do titular das informações (BRASIL, 2011).

Logo, em 30 de novembro de 2012, sancionou-se a Lei 12737, popularmente conhecida como a Lei de Crimes Cibernéticos, dispondo sobre a tipificação de delitos cometidos através da internet e altera o Código Penal Brasileiro (VIANA, 2018).

As sanções aplicadas por esta lei vão desde a pena de detenção, que varia de três meses a dois anos de reclusão, com um agravante de aumento de pena conforme o prejuízo econômico causado, divulgação e vazamento de dados na internet, conteúdos obtidos ligados às comunicações eletrônicas privadas, privacidade comercial e industrial, informações sigilosas e invasão por controle remoto não autorizado a aquele determinado disposto (PINHEIRO; HAIKAL, 2016).

Sendo assim, Vinicius Borges Fortes (2016) ressalta que o legislador passou a dar uma maior proteção aos dados pessoais, estabelecendo como crime a invasão de dispositivos informáticos para obter, adulterar ou destruir informações sem autorização do titular

1.1.1.1 Papéis das inteligências artificiais nas plataformas digitais comerciais

Para Vanessa Araújo de Sant'ana (2015), foi a partir do advento da *World Wide Web* (WWW) ou somente WEB, que a internet ganhou forças e revolucionou o mundo, propondo novas formas de fazer negócios que ganharam espaço e evoluíam constantemente. O comércio eletrônico ou *E-commerce* evoluiu em consequência destes avanços tecnológicos e da popularização da internet.

Todo o processo de negociação em um ambiente eletrônico, por meio da utilização intensa das tecnologias de comunicação e de informação pode ser denominado de comércio eletrônico.

Os autores Euri Charles Andrade da Silva e Tales Vital (2010) evidenciam que, para as vendas de produtos pela internet, as empresas utilizam *websites*, normalmente com um *layout* interativo e de fácil manuseio pelo consumidor. Geralmente, estes *websites* são criados por empresas terceirizadas que desenvolvem um *software*, sendo esta outra forma de comércio eletrônico, denominada como B2B, ou *Business to Business*, no português, de empresa para empresa.

Nesta linha de raciocínio, as empresas consideradas como gigantes da tecnologia, *Amazon, Apple, Facebook, Google, IBM, Microsoft, Tesla, Uber,* dentre outras, se veem numa verdadeira corrida para dominar o mercado, imprevisível em razão da velocidade em que se decorrem os avanços tecnológicos (HOFFMANN, 2018).

O conceito de Inteligência Artificial (IA) abrange mais do que a inteligência da máquina. Pretende-se, com a mesma, capacitar o computador para um comportamento inteligente. Por este comportamento inteligente, deverão ser compreendidas atividades que somente um ser humano poderia ser capaz de efetuar. Dentre estas atividades, podem ser citadas aquelas que envolvem tarefas de raciocínio (planejamento e estratégia), percepção (reconhecimento de imagens, sons, etc) e/ou ainda, no que diz respeito à temática, o *E-commerce* (NORVIG; DUSSEL, 2013).

Pode ser destacado como exemplo de inteligências artificiais, segundo Buchanan e Zimmer (2018) que atualmente a IBM, empresa de informática, atua em várias áreas de publicidade, perfis de consumo, educação, serviços financeiros, dentre outros. Oferece também vários serviços por meio da plataforma da IBM *Cloud*, como os *softwares* de assistência pessoal, análise das informações não-estruturadas, dispositivos de reconhecimento visual, tradutor de linguagens, dentre outros.

Outro exemplo de inteligência artificial, voltada para a área da saúde, desenvolvida pela Microsoft e aplicada no Hospital 09 de Julho. A partir destas redes neurais profundas para compreender determinadas cenas, a análise de filmagens de pacientes idosos internados, favoreceu que o hospital reduzisse rapidamente o número de quedas dos leitos (HOFFMANN, 2018).

Ademais, no âmbito dos transportes, avanços significativos acontecem por meio do desenvolvimento de carros autônomos e sustentáveis. No ano de 2016, a *Tesla Motors*, chefiada por Elon Musk, anunciou que todos os carros produzidos a partir daquele período sairiam equipados com um sistema capaz de conduzir veículos sem qualquer interferência de um humano, ou seja, única e exclusivamente controlada por uma inteligência artificial.

Em outro cenário, no que se refere à contribuição da Inteligência Artificial para as plataformas digitais que o consumidor brasileiro possui acesso, e sabendo das infinitas possibilidades de acesso a esses ambientes virtuais, não seria diferente o avanço frente aos *marketplaces*, afinal eles nada mais são do que tecnologias responsáveis por mediar a ponte entre o vendedor que possui a oferta e o consumidor que detém a demanda (RATZ, 2019).

Ainda segundo Leandro Ratz (2019), o *marketplace* não somente utiliza como também constitui uma Inteligência Artificial. Com isto, a IA utilizada controla esta demanda, ou seja, realiza a ponta, abrindo uma nova oportunidade de receita. Deste modo, podem ser citadas dentro do cenário nacional de plataformas digitais que realizam o uso da IA, o *Facebook Marketplace* e o *Marketplace* Mercado Livre.

Dessa forma, acredita-se que as inteligências artificiais podem alterar fundamentalmente o modo com que os consumidores fazem compras, especificamente com relação às oportunidades facilitadas entre compradores e vendedores, sobretudo nos *marketplaces*.

Conclui-se, portanto, que as inteligências artificiais estão tornando o ambiente E-commerce mais eficaz e personalizado de acordo com cada comprador.

Além de, consequentemente, ajudar vendedores e empresários a comunicarem com mais rapidez ao público alvo.

Entretanto, confirma-se que as mudanças geradas por essas novas tecnologias deverão ser tratadas de forma elucidativa pelo Direito Pátrio. Em razão das constantes alterações nas formas de negócios virtuais, o Direito deverá agir fundamentalmente no que tange à regulação destes meios, com enfoque direto à proteção do consumidor brasileiro.

1.1.1.1.1 Regulação e regulamentação

Ultrapassada a contextualização histórica pertinente à temática, os conceitos necessários para a sua compreensão e efetiva aplicação dos dados pessoais, fica claro a ampla utilização e necessidade de regulação quanto ao uso dos dados pessoais do consumidor.

Logo, a proposta de um conjunto normativo de caráter civil para regulamentar os direitos e responsabilidade inerentes à utilização das plataformas digitais, se tornou fundamental quando envolvia questões que abrangiam o baixo *enforcement* e a insegurança jurídica, ganhando espaço nos debates internacionais de neutralidade e governança de internet (ROCHA, 2017).

Relativo à situação legislativa brasileira atual acerca da proteção de dados, podemos citar como um dos principais expoentes o Marco Civil da Internet.

De acordo com Carlos Afonso Souza e Ronaldo Lemos (2016), a Lei nº 12965/14, mais conhecida como Marco Civil da Internet, se deu após uma consulta pública, na internet, no ano de 2009. Este projeto de lei passou pelo controle e revisão de vários setores da sociedade, entre empresas, organizações da sociedade civil, ativistas e comunidade técnica.

De acordo com o disposto, o objetivo que estimulou a criação da norma civil para as relações sociais e profissionais no ciberespaço tornou-se um estabelecimento de princípios e garantias, como também, direitos e deveres, por meio de procedimentos e dispositivos que possam suprir a ausência de uma legislação

especifica para as questões de natureza cibernéticas (SEGURADO; LIMA; AMENI, 2017).

Deve ser ressaltado que o ambiente digital engloba um amplo panorama de usuários e interesses controversos, além de compreender dentro de sua configuração, posicionamentos distintos sobre a liberdade de funcionamento do ciberespaço e sua arquitetura de colaboração, cuja finalidade, favorece a liberdade de expressão de seus usuários (SEGURADO; LIMA; AMENI, 2017).

A atenção do Estado sobre as relações sociais e econômicas na rede se converte na necessidade para resguardar juridicamente a dignidade e segurança dos usuários. Esta circunstância foi brevemente amparada pelas normas penais, conforme exemplifica, por exemplo, a Lei nº 12737 de 30 de novembro de 2012 (TOMAS; VINICIUS FILHO, 2016).

No entanto, alguns autores se posicionam doutrinariamente, controversos à aprovação de regimes penais de regulamentação de práticas digitais, antes que os dispositivos e previsões de responsabilidade civis estejam esgotados. Em seguida, nota-se a pretensão legislativa em tornar territorialmente regulamentado, um ambiente virtual de escala internacional (TOMAS; VINICIUS FILHO, 2016).

Carlos Afonso Souza e Ronaldo Lemos (2016) apontam que o Marco Civil versou acerca da responsabilidade civil dos provedores de conexão e provedores de aplicação e neutralidade da rede.

Embora a norma penal mencionada, precipitada à margem da Lei nº 12737, também conhecida como “Lei Carolina Dieckmann”, representa um passo audaz na revolução do Direito Digital. Ao se inserir nesta conjuntura, o Marco Civil da Internet, passou a contemplar alguns quesitos anteriormente negligenciados por meio do ordenamento jurídico, com relação ao ciberespaço, como: a liberdade de opinião, a proteção de privacidade de usuários e a neutralidade dos servidores (ROCHA, 2017).

Segundo Ana Cláudia Hostert (2018), o Marco Civil preconiza alguns princípios no que diz respeito ao uso da internet no Brasil em seu artigo 3º, que dispõe

sobre a disciplina do uso da internet no Brasil que tem como princípios a garantia da liberdade de expressão, comunicação e pensamentos.

A Constituição Federal confere proteção da privacidade e do uso de dados, abrange sobre a neutralidade e estabilidade da rede, através de medidas técnicas compatíveis com os padrões internacionais e a estimulação de boas práticas.

Por conseguinte, a responsabilização dos agentes com suas atividades deve propiciar a preservação da participação na rede, bem como auxiliar na liberdade de negócios por meio da internet desde que não vá contra os princípios estabelecidos em Lei.

Para Victor Hugo Pereira Gonçalves (2017), o Marco Civil separou a privacidade de proteção de dados pessoas, mesmo com a estrita ligação que possui. Tal cisão pode até ser interpretada como não constitucional.

Todavia, o Marco Civil, em seu Artigo 7º, apresenta os direitos dos usuários, reforçando a essencialidade de que sejam assegurados os direitos de privacidade e proteção, e caso sejam violados será cabível indenização. Os fluxos de usuários pela internet deverão ser salvos em banco de dados apenas com ordem judicial e as informações armazenadas serão sempre sigilosas. As informações que constam no contrato de prestação de serviços de internet também devem ser advindas de conexão protegida e gerenciamento de redes que não facilite o fornecimento de dados pessoais dos usuários a terceiros (HOSTERT, 2018).

Sendo assim, independentemente da origem do conteúdo acessado, uma vez que, estão previstas algumas discriminações de tráfego decorrentes de requisitos técnicos que são indispensáveis para a prestação correta dos serviços e aplicações, além de priorização dos serviços de emergência (ROCHA, 2017).

Desse modo, sob a ótica de Victor Hugo Pereira Gonçalves (2017), mesmo com a preferência do legislador pela defesa do usuário, há uma falta de transparência nos procedimentos das guardas de dados pessoais pelas empresas de aplicação à internet, e o Marco Civil também não os delimita. Nesta seara, não é possível garantir

direitos sem que existam regras claras e bem definidas sobre como funcionam os sistemas de tecnologia de informação e comunicação.

No entanto, José Luiz Bolzan de Morais e Elias Jacob de Menezes Neto (2014) fazem críticas ao Artigo. 3º do Marco Civil, que são: primeiramente (a forma reducionista de como é tratada a questão de privacidade, apenas como um sinônimo de vida particular, isto é, intromissão nas comunicações privadas armazenadas), segundo (os problemas oriundos da modernidade líquida e que não são resolvidos partindo de soluções independentes da territorialidade, como é o caso do marco civil).

Em outra vertente, o Artigo 8º da referida Lei confere a possibilidade de anulação de cláusulas contratuais que violem os direitos de privacidade e liberdade de expressão em comunicações e dispõe que o direito à privacidade e liberdade de expressão nas comunicações devem ser assegurados. Todavia, só serão nulos esses direitos caso se aplique a ofensas e vá contra o sigilo das comunicações privadas na internet e caso o contrato de adesão não proporcione ao cliente uma alternativa para a adoção do foro brasileiro que solucione essas controvérsias (GONÇALVES, 2017).

Frente a este contexto, a necessidade de cautela na guarda e manuseio dos dados de registros dos usuários decorre, porquanto, não sendo apenas importante protege-los formalmente, mas também materialmente e a partir dos procedimentos de segurança e privacidade.

Cabe esclarecer também que neste tópico foram discutidos somente os artigos pertinentes dentro da mencionada Lei e que foram relevantes de forma direta ao assunto abordado no decorrer deste trabalho.

Sendo assim, André Zonaro Meneguetti e Pamela Gabrielle Giacchetta (2014, p. 390) enfatizam que:

> Ainda que o Marco Civil da Internet contenha alguns dispositivos e princípios esparsos e genéticos relacionados ao tema, a inexistência de um diploma legal especifico sobre a proteção de dados pessoais, é, frequentemente, um empecilho à efetividade do princípio constitucional da intimidade e da vida privada (artigo 5º, inciso X, da Constituição Federal), assim como para a correta e clara delimitação das atividades e ações que são permitidas, desde que consentidas pelos usuários.

Por conseguinte, percebe-se que o Marco Civil traz em seu escopo alguns princípios e diretrizes relativos à proteção dos dados pessoais, todavia, não os regulariza da forma correta, havendo ainda muitas lacunas que transparecem à insegurança dos usuários. Atingindo, principalmente a esfera dos Direitos do consumidor aplicados ao *E-commerce*.

2 Direito Digital e a Lei De Proteção De Dados

2.1 A transparência algorítmica no manuseio de dados pessoais

Conforme evidenciado ao longo desta pesquisa, os dados pessoais possuem alto valor econômico uma vez que traça diversos perfis de consumidores, que por sua vez, se caracteriza como peça-chave para empresas, sendo um veículo capaz de proporcionar maiores lucros para quem tem acesso a essas informações pessoais. Diante da era informacional que estamos vivendo, faz-se importante ressaltar a relevância dos algoritmos na relação de captação de dados.

Marco Medina e Cristina Ferting (2006) denotam que o termo algoritmo é utilizado em diversas áreas, dentre as quais pode-se citar a engenharia, a computação, a administração, dentre tantas outras. Sua definição consiste em ser um procedimento com passo a passo para solucionar um conflito e até mesmo uma sequência detalhada de ações a serem executadas para realizar uma tarefa, desde que seja finito.

Júlio Napoleão de Barros (2020) elucida que o uso massivo de dados pode acarretar em práticas discriminatórias e abusivas, oriundas de processos que não são transparentes. Tendo em vista que num cenário onde as máquinas são programadas para aprenderem sozinhas, há que se falar num aprendizado vulnerável e com pontos cegos. A transparência é um objetivo necessário e de difícil obtenção, principalmente porque a população não detém conhecimento sobre o modo pelo qual as informações podem ser interpretadas e unificadas, ignorando também a intensidade e abrangência dos riscos que essas coletas possuem.

Segundo Júlio Napoleão de Barros (2020) aborda ainda que os indivíduos são influenciados ao longo da sua vida e muito dessa influência decorre dos dados que ele disponibilizou. Tudo isso demonstra que esse mesmo indivíduo é privado de outros

conhecimentos e vivências ao logo de sua existência, principalmente porque os algoritmos estimulam o sujeito baseado somente nas informações que ele fornece, limitando-o e ocultando-o de outros mundos.

Bruna Pinotti Garcia Oliveira (2020) disserta sobre a *Learning Machine* ou aprendizagem de máquina, termo empregado pelo professor Pedro Domingos para abordar a evolução dos algoritmos. E foi através destas sequências de instrução que se chegou ao *Big Data* sendo possível que o algoritmo se desenvolvesse sozinho, dispensando uma programação específica, ou seja, desenvolvendo a si mesmo. Tal desenvolvimento poderá chegar ao que se considera algoritmo mestre, que substitua os diversos tipos de algoritmo e possa derivar dele, todo conhecimento do mundo, envolvendo passado, presente e futuro, mas, ainda está distante da realidade.

A aprendizagem de máquina atua com uma modelagem de padrões, o que compõe uma subárea da inteligência artificial. Esses algoritmos processam os dados dos usuários a fim de direcionar as suas escolhas, quanto a pessoas, gostos musicais, compras, filmes e tudo que seja do interesse daquele indivíduo. Todavia, a sensação de escolha corresponde a 0,1% quando na verdade já estava tudo sendo direcionado para que o indivíduo pudesse “escolher” (OLIVEIRA, 2020).

Os algoritmos permitem que seja criado um perfil desse usuário, essa técnica, conhecida como *profiling* cria uma espécie de representação virtual do indivíduo. Essa técnica se baseia em dados sensíveis, em que contém informações específicas como raça, orientações políticas e religiosas, bem como opções sexuais, fatores que podem enfatizar a discriminação social. Por isso se faz importante uma legislação que zele por questões primordiais como estas, haja vista o que preceitua o artigo 6º da Lei Geral de Proteção de Dados, segundo o qual, deve-se conferir garantia aos titulares, exatidão, clareza, relevância e atualização de dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (OLIVEIRA, 2020).

2.1.1 Conceitos e princípios norteadores da LGPD

Os conceitos que circundam a Lei Geral de Proteção de Dados referem-se principalmente aos sujeitos que estão envolvidos no tratamento de dados, bem como os tipos de dados regulados pela referida lei e os princípios que norteiam o aparato

legislativo. Estes visam proporcionar maior clareza e perfazem todos os pontos importantes dessa relação.

Para Luísa Campos Faria (2019), existem definições relevantes para o correto e amplo entendimento relacionado às obrigações concernentes à atividade normativa. A começar pelo titular, em que se considera pessoa natural a que se referem os dados pessoais em tratamento. O controlador por sua vez, é a pessoa física ou jurídica de direito público ou privado que atua na coleta de dados pessoais, bem como, atua na tomada de decisões em relação a forma e a finalidade do tratamento de dados. Sua responsabilidade consiste em como os dados são coletados, por quanto tempo são armazenados e para que estão sendo utilizados.

No que diz respeito ao operador, este é a pessoa natural ou jurídica, de direito público ou privado que atua na realização do tratamento e processamento de dados pessoais em nome do controlador. O encarregador é designado pelo controlador para atuar como intermediário entre este último, os titulares de dados e a Autoridade Nacional de Proteção de Dados. Essa pessoa tem a função de facilitar a comunicação e garantir o cumprimento das normas de proteção de dados (FARIA, 2019).

Segundo Danilo Doneda (2011), em se tratando dos princípios norteadores da LGPD, há se falar em um “núcleo comum”, caracterizado por um conjunto de medidas que pode ser encontrado em várias normativas que elucidam sobre a proteção de dados pessoais. O referido termo expressa um conjunto de princípios a serem aplicados na proteção dos dados a começar pelo princípio da publicidade (transparência), onde denota que a existência de um banco de dados pessoais deve ser de conhecimento público, exigindo uma notificação prévia para o seu funcionamento.

O princípio da exatidão refere-se ao armazenamento de dados em que estes devem corresponder à realidade, compreendendo a de se fazer uma coleta e tratamento com cuidado e correção. Já o princípio da finalidade preceitua que a utilização dos dados pessoais deve obedecer a uma finalidade, onde se deve comunicar o interessado antecipadamente sobre a coleta de seus dados. Este

princípio é de suma importância, uma vez que a partir dele fundamenta-se a restrição da transferência de dados a terceiros (DONEDA, 2011).

Ademais, o princípio do livre acesso elucida que o indivíduo tenha acesso ao banco de dados em que suas informações estejam armazenadas, permitindo que ele tenha cópias dos registros, bem como a possibilidade de controlar esses dados, efetuando inclusive, possíveis correções em suas informações. No que se referem ao princípio da segurança física e lógica, os dados devem ser protegidos contra transmissão ou acesso não autorizado, destruição, extravio ou modificações (DONEDA, 2011).

Segundo Sérgio Ricardo Correia de Sá Junior (2018), o princípio da não discriminação, que também se encontra na regulamentação europeia reforça ideia de que a proteção de dados pode causar danos diversos uma vez que não tenha sido abordada de forma correta. Tais danos consistem na perda de controle dos dados pelo titular, bem como discriminação e roubo de identidade. Diante disso, uma vez que o controlador identifique houve uma violação, ele deve comunicar as autoridades.

Os princípios da LGPD se correspondem com os princípios da GDPR, estes que são a base de diversas leis e perfazem o ordenamento jurídico. Diante disso é importante denotar alguns impasses entre tais princípios e a aplicabilidade da lei, a fim de ir aprimorando e sanando eventuais conflitos, garantindo o bem maior que é a segurança de dados pessoais.

2.1.1.1 Lei Carolina Dieckmann

Em maio de 2011, um hacker invadiu o computador pessoal da atriz Carolina Dieckmann, tendo acesso a múltiplas fotos da atriz de cunho íntimo. O criminoso chantageou a artista, exigindo uma quantia em dinheiro para não divulgar as fotos online. Após a recusa da atriz, todas as imagens foram publicadas na internet, gerando um alvoroço virtual.

Todo o acontecido criou uma discussão em volta dos crimes cibernéticos, e como não havia normas em torno desses problemas que estavam sendo cada vez mais comuns no poder jurídico. Esse debate popular, fomentado pela mídia,

pressionou o sistema judiciário brasileiro a tipificar crimes cometidos no ambiente virtual.

Carolina Dieckmann mergulhou no movimento, e, como resultado, o projeto da Lei Carolina Dieckmann foi aprovado em um tempo recorde de pouco mais de um ano. A Lei Nº 12.737/2012 é uma alteração no Código Penal Brasileiro voltada para crimes virtuais e delitos informáticos, com foco nas invasões de computadores e outros eletrônicos sem a permissão do dono, e se tornou um marco para o Direito Digital. Segue abaixo uma transcrição:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (“L12737 - Planalto”)
>
> "§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:" (“L12737 - Planalto”)
>
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”
>
> “Ação penal
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.”
> Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação: “Interrupção ou

> perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
>
> Art. 266 § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (“L12737 - Planalto”) § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
>
> Art. 298 Falsificação de cartão Parágrafo único. "Para fins do disposto no caput , equipara-se a documento particular o cartão de crédito ou débito.”" (“L12737 - Planalto”) (NR)

Ela impacta o Direito Penal, pois acrescenta os artigos 154-A e 154-B ao Código Penal Brasileiro. E também muda a redação dos artigos 266 e 298. A norma em questão aborda uma tendência do Direito que se refere à segurança no ambiente virtual, tendo em vista que seu texto contempla as práticas criminiosas derivadas do uso impróprio de informações e materiais pessoais, tais como fotos e vídeos, que são relevantes para a privacidade de um indivíduo na internet.

Mesmo que seja um consenso público a necessidade de zelar pela segurança da privacidade em contextos online, a Lei Carolina Dieckmann levanta vários debates. Um deles é o fato de o texto ser essencialmente vago e carecer de aspectos técnicos.

Por exemplo, é incerto se a violação de um dispositivo eletrônico de propriedade do próprio usuário constitui um delito. Esse aspecto pode suscitar diferentes opiniões entre os profissionais do Direito, o que gera incertezas jurídicas em casos concretos.

Adicionalmente, um problema adicional reside no fato de que a lei não especifica claramente quais tipos de dispositivos eletrônicos são abarcados pela norma, deixando margem para interpretação por parte das autoridades do Poder Judiciário e do Ministério Público. Embora a Lei Carolina Dieckmann tenha sido um marco inicial na proteção dos dados pessoais dos cidadãos contra ataques virtuais, verifica-se que ainda é necessário um processo de amadurecimento normativo para eliminar ambiguidades em sua aplicação.

2.1.1.1.1 MARCO CIVIL DA INTERNET

Em uma publicação feita no dia 24 de março de 2014, o site World Wide Web Foundation divulgou um pronunciamento de Sir Tim Berners-Lee, já apontado nesta monografia como inventor da internet na forma que conhecemos hoje, que

demonstrou grande entusiasmo com a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), conforme segue a publicação de World Wide Web Foundation (2014)

> Se o Marco Civil for aprovado, sem maiores adiamentos ou modificações, este seria possivelmente o melhor presente de aniversário para os usuários de internet do Brasil e do mundo. Eu espero que, aprovando esta lei, o Brasil fixe sua orgulhosa reputação como um líder mundial em democracia e progresso social e ajude a inaugurar uma nova era, uma onde os direitos dos cidadãos em todos os países do mundo são protegidos por leis de direito digitais.

Além disso, para Sir Tim Berners-Lee, no mesmo pronunciamento, a legislação "reflete a internet como deveria ser: uma rede aberta, neutra e descentralizada, onde os usuários são o motor para a colaboração e inovação" (World Wide Web Foundation, 2014).

De fato, neste tópico ficará demonstrado como o Marco Civil da Internet se preocupou em abordar diversos direitos, garantias e deveres relativos à rede mundial de computadores, com foco a ser explorado, aqui, nas inovações com relação ao direito fundamental à privacidade online.

Nesse sentido, é o que informa Teixeira (2016, p. 84)

> Preocupado com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários da internet, o Marco Civil expressa que a garantia a esses dois direitos constitucionais é condição para o pleno exercício do direito à acesso à rede mundial de computador. Ou seja, a violação a esses direitos implica em quebra da própria finalidade do advento do Marco Civil enquanto uma lei federal que objetiva tutelar os usuários da internet.

Logo em seu artigo 3º, incisos II e III, o Marco Civil da Internet já estabelece, como princípios do uso da internet no Brasil, dentre outros, a "proteção da privacidade" e a "proteção dos dados pessoais, na forma da lei" (BRASIL, 2014), sendo que a proteção dos dados pessoais, conforme Teixeira (2016), não foi tratada de forma tão específica nesta norma, devendo ser disciplinado por uma lei posterior (no caso, a lei n. 13.709 de 14 de agosto de 2018, ou Lei de Proteção de Dados Pessoais, que será abordada em um tópico adiante).

Posteriormente, no artigo 7º, incisos I, II, III, VII, VIII, IX e X, é mais específica a legislação quanto aos direitos relativos à privacidade conferidos aos usuários de internet, garantindo, no primeiro inciso, a "inviolabilidade da intimidade e da vida privada", no segundo, a "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei" e, no terceiro, a "inviolabilidade e

sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial” (BRASIL, 2014).

É importante ressaltar que, neste ponto da lei, surge a expressão “salvo por ordem judicial”, indicando que a inviolabilidade assegurada não é absoluta, podendo ser derrubada em alguns casos específicos, abrindo margem para uma discussão de suma importância acerca do interesse público do Estado para a prestação da tutela jurisdicional e garantia da segurança pública contra o direito de privacidade na rede, que será abordada nesta monografia em tempo oportuno.

Seguindo o raciocínio dos primeiros três incisos do art. 7º, segue o entendimento de Teixeira (2016, p. 69)

> Assim como nas questões fiscais, bancárias, etc. o fluxo das comunicações pela internet são sigilosas e invioláveis. Nestes casos, apenas por ordem judicial, conforme a legislação a ser editada, poderá decretar a quebra do sigilo das comunicações eletrônicas estabelecidas pela internet.

Ainda, é na mesma linha o texto publicado pela Academia Brasileira de Direito do Estado – ABDET (2015, p. 7)

> No mesmo sentido, a guarda de dados e informações dos usuários da internet prevista nessa lei deve ser realizada com a estrita observância das regras constitucionais de preservação da intimidade, sendo passíveis de serem reveladas somente através de ordem judicial.

Desta forma, evidente que a proteção ao sigilo das comunicações privadas no âmbito da internet é imprescindível, conforme a legislação citada, pois garante o direito à privacidade dos usuários, observando-se o dever de indenizar, moral ou materialmente, os danos causados por aquele que viola este direito.

Dando sequência, nos incisos VII, VIII, IX e X do artigo 7º do marco regulatório, são indicados alguns direitos relativos à proteção dos dados dos usuários, sendo que muitos destes incisos carecem de eficácia por conta da necessidade de uma lei que os regulamente, carência esta que será suprida quando entrar em vigência a Lei de Proteção de Dados Pessoais, conforme será abordado em um tópico posterior.

Seguem os enunciados do artigo e dos incisos referidos acima (BRASIL, 2014)

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

(...)

"VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;" (“Art. 7 da Lei 12965/14 | Jusbrasil”)

"VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:" (“L12965 - Planalto”)

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

"IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;" (“Art. 7, inc. IX da Lei 12965/14 - jusbrasil.com.br”)

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

Percebe-se que todos estes incisos se referem aos dados pessoais dos usuários e traçam linhas gerais para o devido tratamento desses dados por parte dos provedores de acesso e de aplicações de internet. O inciso VII aponta a impossibilidade de fornecimento de dados a terceiros sem consentimento expresso, o VIII cita que há uma necessidade de transparência na relação de tratamento dos dados coletados com os usuários, o inciso IX, por sua vez, trata da exigência de consentimento expresso em cláusula contratual destacada e, por último, o inciso X informa, na descrição feita pela Academia Brasileira de Direito do Estado – ABDET (2015, p. 9), que “O usuário que deseje contratar com outra Prestadora poderá requisitar ao antigo provedor que não mantenha seus dados pessoais nos registros”.

Desta forma, já no Marco Civil da Internet foram estabelecidos diversos direitos no sentido da proteção de dados pessoais, demonstrando uma preocupação e a necessidade de uma legislação com a finalidade de proteger a vida privada dos usuários, assunto que será aprofundado posteriormente, quando a Lei de Proteção de Dados Pessoais for analisada.

No artigo 8º do marco regulatório, é positivado o entendimento que “a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet” (BRASIL, 2014), concluindo-se, então, nas palavras da Academia Brasileira de Direito do Estado – ABDET (2015, p. 10) que

> Os provedores responsáveis deverão proteger os registros, dados pessoais e as comunicações privadas dos usuários, cuja finalidade é a preservação da intimidade, da privacidade, da honra e da imagem dos usuários, sendo que a divulgação de tais informações se dará apenas através de ordem judicial, ressalvada a possibilidade das autoridades administrativas obterem os dados cadastrais, na forma da lei.

Destarte, quanto ao supracitado, “qualquer pacto celebrado entre as partes, ou mesmo termos de uso, que viole o direito à privacidade e à liberdade de expressar-se do usuário é nulo de pleno direito”. (TEIXEIRA, 2016, p. 84).

O Marco Civil também determinou, no parágrafo único, inciso I, do artigo 8º, que as cláusulas contratuais que impliquem “ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet” (BRASIL, 2014) são nulas de pleno direito, ou seja, expressamente indicou que tal sigilo tem tanta importância no ordenamento jurídico que deve ser um direito indisponível, isso porque ninguém deve ser constrangido a aceitar esta violação em troca de, por exemplo, a utilização de um serviço, salvaguardando o usuário de práticas comerciais abusivas que visem condicionar o uso de uma aplicação de internet a uma contraprestação desproporcional, qual seja a invasão de privacidade caracterizada pelo violação do sigilo das comunicações privadas dos usuários.

O Marco Civil da Internet segue, no artigo 10, discorrendo sobre a proteção dos registros de conexão, comunicações e dados dos usuários, ao citar que

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da

> intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
>
> "§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o." (“neutralidade de rede e liberdade de expressão - Jusbrasil”) 34
>
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. (“LEI Nº 9 - camara.leg.br”) (BRASIL, 2014).

Válido destacar, neste artigo, que apesar de ser reforçada a custódia do direito à privacidade, são levantadas hipóteses mais concretas da não aplicação ou do rompimento destes direitos, seguindo o que já havia sido visualizado nos incisos II e III do artigo 7º. Dessa vez, o Marco Civil remete aos artigos 22 e 23 do seu texto, que exploram a possibilidade de requerimento ao juízo durante o curso de uma ação cível ou penal para que seja ordenado aos provedores o fornecimento dos registros relacionados a determinados indivíduos.

Nessa linha, conforme a Academia Brasileira de Direito do Estado – ABDET (2015), enquanto os §§ 1º e 2º tratam da necessidade de uma ordem judicial para a disponibilização de dados pessoais e de seu conteúdo, o § 3º classifica-se como uma exceção à regra, que seria a imprescindibilidade da ordem judicial, informando que os dados de qualificação pessoal contidos no dispositivo podem ser obtidos através de uma mera requisição feita pelas autoridades administrativas, levando em conta que, conforme o art. 11, § 3º, do Decreto n. 8.771, de 11 de maio de 2016, o qual regulamentou o Marco Civil da Internet, é vedado que os pedidos desse gênero sejam, quando coletivos, inespecíficos ou genéricos. Entretanto, a legislação não é clara quanto a especificação das autoridades administrativas competentes para fazer esta requisição.

Quanto ao artigo 11, já citado no tópico da transnacionalidade da rede, é importante destacar o § 3º, que indica que

> § 3º e Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. (BRASIL, 2014).

A regulamentação referida neste artigo chegou ao ordenamento jurídico brasileiro através do Decreto n. 8.771, de 11 de maio de 2016, o qual, entre outras questões, estabeleceu alguns padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, como os elencados no artigo 13, incisos I a IV, do seu texto

> Art. 13. "Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:" (“Decreto nº 8771 - Planalto”)
>
> "I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;" (“Decreto nº 8771 - Planalto”)
>
> II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; (“Decreto nº 8771 - Planalto”)
>
> III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
>
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. (BRASIL, 2016).

Desta maneira, restou claro que o tratamento dos dados pessoais, comunicações e registros dos usuários deve ter padrões de segurança internos no âmbito das entidades que detenham estes registros, como a definição de responsabilidades das pessoas que terão possibilidade de acesso aos dados, mecanismos de autenticação de acesso aos registros, criação de inventário dos acessos feitos pelos funcionários e uso de outras técnicas de gestão dos registros, tudo para assegurar a maior privacidade possível.

Ainda, foi fixado, no § 2º, incisos I e II, do artigo anterior, o seguinte

§ 2o Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:

I - tão logo atingida a finalidade de seu uso; ou (“Termos de Uso | Leadster”)

II - se encerrado o prazo determinado por obrigação legal. (BRASIL, 2016)

Portanto, ao ponto em que encerrar o prazo determinado na legislação para a retenção dos dados e registros, ou quando a finalidade de seu uso for atingida, estes devem ser excluídos, indicando que o tratamento destes dados não tem caráter permanente e irrestrito, sendo o seu uso vinculado à finalidade para que foi captado, com aceite expresso do usuário, e com o tempo de duração do tratamento sendo aquele especificado em lei.

Dando sequência, o artigo 13 do Marco Civil da Internet informa que cabe ao provedor de conexão ou àqueles que possuam um sistema autônomo (como algumas universidades com endereço próprio de protocolo de internet) o dever de manter os registros de conexão em ambiente seguro e sob sigilo pelo prazo de 1 ano, sendo que tal responsabilidade não pode ser transferida para terceiros, e indica a possibilidade da autoridade administrativa, policial ou do Ministério Público requerer a guarda dos registros de conexão por tempo superior.

Para efeitos do artigo anterior, Teixeira (2016, p. 106), define registros de conexão como o “conjunto de informações referentes à data e hora de início e término de uma conexão 36 à internet, sua duração e o endereço IP utilizado pelo terminal para envio e recebimento de pacote de dados”.

Desta forma, válido ressaltar, conforme Teixeira (2016), que o mero compartilhamento de rede Wi-Fi feita por estabelecimentos empresariais não significa que eles têm o dever de guardar os registros de conexão, uma vez que, geralmente, estas empresas não possuem um sistema autônomo, e sim uma rede considerada como uma única conexão identificada pelo mesmo protocolo de internet (IP) para o provedor de conexão.

Importante destacar, também, o artigo 14 do marco regulatório, que cita que “na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet” (BRASIL, 2014). Nessa linha, a Academia Brasileira de Direito do Estado – ABDET (2015, p. 15), cita que

> O legislador vedou expressamente ao provedor de conexão guardar sob sigilo os registros de acesso a aplicações da internet, ficando tal obrigação a cargo do provedor de aplicações, que deverá constituir pessoa jurídica regular e manter os dados pelo prazo de 6 meses, conforme o artigo 15.

Já no artigo 15, conforme o Marco Civil

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

É importante frisar aqui que os registros de acesso a aplicações de internet, no conceito de Teixeira (2016, p. 113) “tratam-se do conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço de IP”.

Além disso, de acordo com o mesmo dispositivo, no § 1º, provedores de aplicações de internet que não estão sujeitos ao disposto no caput podem ser obrigados, mediante ordem judicial, a guardarem registros de acesso a aplicações de internet relativos a fatos específicos em um período determinado; no texto do § 2º, pode ser requerido por autoridade administrativa, policial ou pelo Ministério Público, cautelarmente, a qualquer provedor de aplicações de internet, que estes registros sejam guardados por prazo superior ao previsto. Ademais, no § 3º consta a informação que, em qualquer hipótese, no âmbito do artigo 15, deve haver uma autorização judicial que preceda qualquer disponibilização dos registros ao requerente

Portanto, restou estabelecido, para auxiliar na prestação da tutela jurisdicional na rede mundial de computadores, mesmo que implicando em uma limitação do direito fundamental à privacidade, que os provedores de conexão à internet devem guardar os registros de conexão pelo prazo de um ano e que os provedores de aplicações de internet que exerçam atividade empresarial (ou até mesmo os que não exerçam, desde que seja determinado por ordem judicial), devem guardar os registros de acesso a aplicações de internet pelo prazo de 6 meses, como regra geral.

Essencial se faz a breve análise, também, do artigo 16, incisos I e II, do Marco Civil da Internet, que visa a proteção da privacidade em duas vertentes ao afirmar que

> Art. 16. "Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:" (“Art. 16 da Lei 12965/14 - Jusbrasil”)
>
> I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou (“Art. 16 da Lei 12965/14 - Jusbrasil”)
>
> "II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular." (“L12965 - Planalto”) (BRASIL, 2014).

Com efeito, tais vedações reforçam os enunciados do artigo 7º, incisos VII e IX, do marco regulatório, já abordados neste trabalho. Conforme Teixeira (2016), esse reforço está ligado principalmente à ideia de proteção contra o marketing eletrônico, nos casos em que, por exemplo, sites de busca efetuem o armazenamento de informações dos usuários que utilizam a aplicação, visando vender essas informações para empresas que queiram divulgar seus produtos para estes próprios usuários, sem que tenha havido consentimento prévio para tal prática.

Em síntese, foram suscitados os principais institutos do marco regulatório com relação ao direito à privacidade, representando, como o próprio nome da lei sugere, um marco histórico na busca não só pela efetiva prestação da tutela jurisdicional no âmbito do mundo digital, mas também pela consolidação de direitos, deveres e conceitos importantes para definir juridicamente aspectos relacionados à internet, aos usuários, aos provedores e ao Estado. Desta maneira, passaremos então à análise da Lei n. 13.709, de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados – LGPD

2.2 Lei Geral de Proteção de Dados LGPD

Nós vivemos em um mundo onde, há um bom tempo atrás, as empresas viam todas as pessoas como iguais. Então, se existisse um grupo de pessoas, uma empresa via esse grupo de pessoas como pessoas iguais. Ela entendia que todo mundo tinha os mesmos gostos, as mesmas vontades, os mesmos desejos. Só que o tempo foi passando e as empresas perceberam que não era eficiente olhar todo mundo como um grupo de pessoas iguais. E essas empresas poderiam descobrir como separar esses grupos através de dados. Esses dados se tornaram informação, nossas informações. Um conhecimento virtual compartilhado da humanidade.

A Lei Geral de Proteção de Dados foi criada para estabelecer as regras do uso de dados. A LGPD, veio, portanto, para dar autodeterminação informativa ao titular sobre os seus dados, tendo o mesmo impacto que o Código do Consumidor teve quando ele surgiu e entrou em vigor. Hoje, para todos nós, é comum falar do código de Defesa do Consumidor, não havendo uma empresa que não observe ele. A LGPD também assume esse caminho, só que, talvez, ainda mais rápido do que foi com Código de Defesa do Consumidor. Estamos falando do principal ativo de toda e qualquer empresa, seja ela ambientada online ou offline, seja ela um MEI (um microempreendedor individual), seja ela uma multinacional. Estamos falando de uma lei que impacta a todos e que é obrigatória para todos. E, sobretudo, que já está em vigor.

> 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 à informação. Em vez de empresas, temos organizações moleculares, baseadas no Indivíduo. A mudança é constante e os avanços tecnológicos afetam diretamente as relações sociais. Portanto, o ramo do Direito Digital é inerentemente pragmático e costuma ser fundamentado em estratégias jurídicas e dinamismo, para poder acompanhar o ritmo acelerado do avanço tecnológico e suas implicações legais (PECK, 2019, p. 74)

Em primeiro lugar, a LGPD determina que os Controladores de Dados indiquem uma figura para o cargo de Encarregado de Dados. A LGPD determina, também, que a figura que ocupa o cargo de DPO deve ser responsável pela interface da empresa ou do órgão público (possíveis controladores) com o titular de dados pessoais e com Autoridade Nacional de Proteção de Dados (ANPD).

Em terceiro lugar, o DPO é o cargo que se responsabiliza por manter a empresa em compliance, ou seja, em conformidade com a LGPD. Então, ele é um cargo extremamente estratégico, porque ele participa, ativamente, de todas as operações da empresa, uma vez que ele vai ter que sempre opinar em relação aos produtos, serviços e processos estabelecidos. O DPO, além de diversas outras funções, determina como algum processo, produto ou serviço está ou não em conformidade com a LGPD.

A LGPD (13.709) foi sancionada em 2018 e os legisladores entenderam que o país precisava de um período de dois anos para que nós pudéssemos nos adaptar. Quando ela foi sancionada, em 2018, o legislador tinha colocado o que o DPO precisava ter “conhecimento jurídico regulatório”. A interpretação que se tirava daquilo

era que o DPO, então, precisaria ser um profissional da área jurídica, uma vez que ele precisava ter conhecimento jurídico regulatório.

Contudo, quando ocorreu a MP que criou a Autoridade Nacional de Proteção de Dados (ANPD) e fez algumas alterações na redação da LGPD, essa parte, de deter "conhecimento jurídico regulatório" foi retirada do texto. Fizeram isso justamente para não nichar a atuação do DPO, para não criar uma oportunidade apenas para os juristas, ou seja, para abranger a oportunidade para mais pessoas.

> A LGPD surge com o intuito de proteger direitos fundamentais como privacidade, intimidade, honra direito de imagem e dignidade. Pode se pontuar também que a necessidade de leis específicas para a proteção dos dados pessoais aumentou com o rápido desenvolvimento e expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder. (PECK, 2020, p. 70)

A LGPD é o passo mais importante tomado por nosso sistema jurídico nesse assunto. O Direito está em constante mudança e evolução de acordo com as necessidades da sociedade, e quanto mais adentramos no ambiente virtual, mais é imprescindível a regulamentação do Direito Digital.

3 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A proteção de dados pessoais no Brasil é garantida pela Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020. A LGPD é inspirada na General Data Protection Regulation (GDPR), da União Europeia, e tem como objetivo proteger os direitos fundamentais de privacidade e liberdade dos indivíduos em relação ao tratamento de seus dados pessoais.

Para Laura Schertel:

> O consentimento não pode ser visto como a única forma de legitimação para o tratamento de dados pessoais. É importante considerar outras bases legais previstas na LGPD, como o cumprimento de obrigação legal ou regulatória e o exercício regular de direitos.

A LGPD se aplica a qualquer pessoa física ou jurídica que realize o tratamento de dados pessoais, desde que esse tratamento seja realizado no Brasil ou tenha como objetivo a oferta de bens ou serviços no país. A lei define dados pessoais como informações que permitem a identificação de uma pessoa natural, direta ou indiretamente, como nome, endereço, CPF, entre outros.

Entre as principais disposições da LGPD estão a necessidade de

consentimento explícito do titular dos dados para o tratamento de seus dados pessoais, a obrigatoriedade de informar de forma clara e transparente sobre a finalidade do tratamento de dados e a garantia de acesso aos titulares aos seus dados pessoais e a correção ou eliminação desses dados.

Além disso, a LGPD prevê sanções para o descumprimento de suas disposições, que podem incluir advertências, multas e até mesmo a proibição do tratamento de dados pessoais. O órgão responsável por fiscalizar o cumprimento da lei é a Autoridade Nacional de Proteção de Dados (ANPD), que tem o poder de aplicar as sanções previstas na LGPD.

Em resumo, a proteção de dados pessoais no Brasil é uma questão importante e a LGPD é um passo fundamental para garantir a privacidade e liberdade dos indivíduos em relação ao tratamento de seus dados pessoais. É fundamental que empresas e outras organizações se adequem às disposições da lei para evitar sanções e proteger a privacidade de seus clientes e usuários.

3.1 DIREITO FUNDAMENTAL À PRIVACIDADE

O direito à privacidade, previsto no art. 5º, inciso X, da Constituição Federal de 1988, tem o seguinte teor “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), e pertence à gama de direitos relativos à personalidade. Foi criado com o intuito de proteger a vida privada dos indivíduos contra a conduta invasiva de outros particulares ou do próprio Estado. Embora tenha suas origens na antiguidade clássica, o conceito de direito à privacidade utilizado nos dias atuais é uma construção recente.

3.1.1 Privacidade online

Com as questões atinentes ao funcionamento da internet e à disseminação de informação, combinadas com o direito fundamental à privacidade, tornam-se evidentes os obstáculos que o Estado enfrenta na tentativa de manter a sua tutela jurisdicional no âmbito digital, seja pela dificuldade no rastreamento dos indivíduos que violam o direito à privacidade, seja pelo caráter transnacional da internet, seja pela elevada velocidade de difusão da informação com a sua característica quase irreversível: uma vez incorporada na rede mundial de computadores, ela não “esquece”.

Leonardi (2011, p. 39) comenta sobre o assunto

> A Internet não exige apenas novas soluções jurídicas para os novos problemas; ela também afeta a maneira como os problemas e as soluções

> jurídicas devem ser analisados. Ao romper com os paradigmas jurídicos tradicionais e desafiar os mecanismos convencionais de tutela, a Rede representa um dos principais objetos de estudo dos doutrinadores preocupados com essa nova realidade social.

Segundo Leonardi (2011), a busca pela solução para resolver os problemas inerentes das características da internet resultou em algumas correntes doutrinárias, quais sejam as de autorregulação, de “direito específico do ciberespaço”, de analogia e de uma abordagem mista com sistema jurídico aliado à arquitetura da internet.

Nas definições de Leonardi (2011), a corrente de autorregulação enfatiza o ciberespaço como um ambiente anárquico, onde os conflitos seriam resolvidos pelos próprios usuários, sem nenhuma interferência governamental; a de “direito específico do ciberespaço” indica que, como a rede mundial de computadores não possui fronteiras no território físico mundial, seria impossível impor a tutela jurisdicional prestada por apenas um Estado, defendendo então a criação de um direito global específico, originado através de uma cooperação internacional para regular as interações no mundo virtual; a corrente de analogia defende que seria viável a regulação da internet apenas aplicando normas e princípios já existentes, de forma análoga nas situações cibernéticas; por último, a corrente de abordagem mista com sistema jurídico aliado à arquitetura da internet, que é a doutrina que prevalece, informa que é possível regular as interações digitais através do direito positivado, mas, além disso, é preciso utilizar-se da própria arquitetura da internet, ou seja, desenvolver tecnologia que opere dentro da rede para garantir a efetividade do direito, combater “fogo com fogo”.

Dentre as legislações nacionais criadas até o presente momento em uma tentativa de prestar a tutela jurisdicional de garantia de privacidade na rede, merecem grande destaque a Lei Carolina Dieckmann (Lei n. 12.737, de 30 de novembro de 2012), o Marco Civil da Internet 29 (Lei n. 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados (Lei n. 13.709, de 14 de agosto de 2018).

Entretanto, importante destacar que o direito à privacidade online não é absoluto, devendo ser analisado, principalmente, observando e respeitando o direito de liberdade de expressão dos indivíduos, de forma a encontrar harmonia para a coexistência dos dois institutos. Tal conflito se mostra bastante evidente, por exemplo, no campo de comentários do perfil de um usuário de alguma rede social, que pode acabar recebendo mensagens que o desagradem, ou até mesmo com empresas de telemarketing que conseguiram dados pessoais de indivíduos de alguma forma e realizam ligações.

Seguindo esta linha, conforme a 2ª Câmara de Coordenação e Revisão do

MPF cita em seu Roteiro de Atuação Sobre Crimes Cibernéticos (2013, p. 336) “A intimidade não é um valor intangível como pregou a mídia no caso motriz da lei. A sua proteção impõe modelação com a liberdade de expressão, sempre para evitar abusos”.

Portanto, é de suma importância reconhecer que existe uma linha tênue para alcançar a justiça ao pesar os direitos à privacidade e à liberdade de expressão no mundo virtual, de forma a garantir que não haja nada no mundo virtual que possa ser considerado invasivo em excesso, tampouco nada que caracterize qualquer forma de censura

CONCLUSÃO

Vivemos em uma era em que a tecnologia está em constante evolução, e as ferramentas digitais se tornaram parte fundamental da nossa vida cotidiana. Com o uso crescente dessas tecnologias, surgiu a necessidade de proteger a segurança digital dos usuários, uma vez que os dados pessoais estão cada vez mais expostos e vulneráveis a ataques cibernéticos.

Os vazamentos de dados, como mencionado no texto, são uma das principais ameaças à segurança digital dos usuários. Eles podem resultar em uma série de problemas sociais, incluindo empréstimos e dívidas de cartões de crédito em nome de terceiros, fotos vazadas de pessoas renomadas e a exposição de dados importantes de ministros e investigações sigilosas. É importante ressaltar que não apenas as pessoas famosas são afetadas por esses vazamentos, mas também pessoas comuns que podem ter suas informações expostas para milhões de pessoas na internet.

Diante desse cenário, é crucial que as empresas que trabalham com ferramentas digitais adotem medidas para garantir a segurança dos dados de seus usuários. O sigilo no cadastro de plataformas e sites de ecommerce é uma dessas medidas, assim como o desenvolvimento de softwares mais precisos e seguros que impeçam o acesso de agentes invasores.

As empresas também precisam ser mais criteriosas na concessão de empréstimos e cartões de crédito, adotando medidas de verificação de identidade mais precisas e seguras. Além disso, treinamentos internos e métodos de identificação diferenciados para cada usuário podem ajudar a diminuir a prática criminosa.

É essencial que a sociedade como um todo reconheça a importância da proteção de seus dados pessoais e que empresas e órgãos governamentais trabalhem juntos para garantir a segurança digital dos usuários. A tecnologia é uma ferramenta poderosa que pode trazer grandes benefícios, mas também pode ser usada para fins mal-intencionados. É responsabilidade de todos garantir que o uso dessas tecnologias seja seguro e responsável.

REFERÊNCIAS

ASSEF, Otávio. **Direito Digital no Brasil Entenda Como Funciona.** Disponível em: https://oa.adv.br/noticias/direito-digital-no-brasil/. Acesso em 01/04/2022

ALVES, Marcelo de Camilo Tavares. **Direito Digital**. Acesso em 01/04/2022.

BRASIL, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Brasília, DF, 2018. Acesso em: 24 de abril de 2023.

BRASIL, LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto- Lei nº 2.848 de 7 de dezembro de 1940, conhecida também como Lei Carolina Dieckman, Brasília, DF, 2012. Acesso em: 24 de abril de 2023

GONÇALVES, Antônio, DE 01 DE OUTUBRO DE 2021, Lei Geral de Proteção de Dados Pessoais, as responsabilidades e os aspectos penais, 2021, Disponivel em: https://www.conjur.com.br/2021-out-01/goncalves-lgpd-responsabilidades-aspectos-penais#:~:text=J%C3%A1%20a%20Lei%20n%C2%BA%2014.155,por%20meio%20de%20dispositivos%20eletr%C3%B4nicos, Acessado em: 24/04/2023

GIRARDELLO, Diogo Prestes. **O Que é Direito Digital?** Disponível em: https://juridicocerto.com/p/advocaciadpg/artigos/o-que-e-direito-digital-1822. Acesso em 02/04/2022.

GONÇALVES, Antônio. **Lei Geral de Proteção de Dados Pessoais, as responsabilidades e os aspectos penais.** Disponível em: https://www.conjur.com.br/2021-out-01/goncalves-lgpd-responsabilidades-aspectospenais#:~:text=J%C3%A1%20a%20Lei%20n%C2%BA%2014.155,por%20meio%20de%20dispositivos%20eletr%C3%B4nicos.Acesso em 01/04/2022

INFOCREDI, **Crimes Cibernéticos devem avançar mesmo com a LGPD**. Disponivel:https://infocredi360.com.br/exclusivos/crimes-ciberneticos-devem-avancar-mesmo-com-a-lgpd. Acesso em 01/04/2022.

MARINHO, Guilherme, Hackers, Crackers e o Direito Penal, 18 de agosto de 2018, Disponivel em: https://www.jusbrasil.com.br/artigos/hackers-crackers-e-o-direito-penal/407334629, Acessado em: 24/04/2023

NUCCI, Guilherme de Souza. **Código Penal Comentado/** – 12. Ed. Rev, atual e amp. – São Paulo: Editora Revista dos Tribunais, 2012

NOVO, Benigno Núñez. **Direito Digita**. Disponível em: https://meuartigo.brasilescola.uol.com.br/direito/direito-digital.htm. Acesso em 02/04/2022

OLIVEIRA, Camila Martins, HORITA, Fernando Henrique da Silva, MORAIS, Fausto Santos de Morais. **Direito Penal e Cibercrimes**. Disponível em: https://conpedi.org.br/wp-content/uploads/2021/07/Livro-10-Direito-Penal-e-Cibercrimes.pdf. Acesso em 01/04/2022

JESUS, MILAGRE, Damásio de, José Antônio. **Manual de Crimes Informáticos** – São Paulo: Saraiva, 2016.

PONTICELLI, Murilo Meneghel. Trabalho de conclusão. Tema: O Direito Fundamental à privacidade no Âmbito da Rede Mundial de Computadores com o Advento da Lei Geral de Proteção de Dados, Faculdade Sul de Santa Catarina, disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/6124/1/TCC%20Murilo%20Assinado.pdf2018, Acesso em: 24/04/2023