UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

MARCELO VANDRÉ RIBEIRO BARRETO FILHO

OS CONTORNOS JURÍDICOS DA LEI GERAL DE PROTEÇÃO DE DADOS FRENTE AO CONSUMO NO AMBIENTE VIRTUAL

SANTA RITA
2019

MARCELO VANDRÉ RIBEIRO BARRETO FILHO

OS CONTORNOS JURÍDICOS DA LEI GERAL DE PROTEÇÃO DE DADOS FRENTE AO CONSUMO NO AMBIENTE VIRTUAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas da Universidade Federal da Paraíba, como exigência parcial da obtenção do Título de Bacharel em Ciências Jurídicas.

Orientador: Prof. MS. Alex Taveira dos Santos

SANTA RITA
2019

Catalogação na publicação
Seção de Catalogação e Classificação

F481c Filho, Marcelo Vandre Ribeiro Barreto.
OS CONTORNOS JURÍDICOS DA LEI GERAL DE PROTEÇÃO DE DADOS FRENTE AO CONSUMO NO AMBIENTE VIRTUAL / Marcelo Vandre Ribeiro Barreto Filho. - João Pessoa, 2019.
50 f.

Orientação: ALEX TAVEIRA DOS SANTOS.
Monografia (Graduação) - UFPB/CCJ.

1. LEI GERAL DE PROTEÇÃO DE DADOS. 2. DADOS PESSOAIS. 3. CONSUMIDOR. 4. INTERNET. 5. DIREITO DIGITAL. I. DOS SANTOS, ALEX TAVEIRA. II. Título.

UFPB/CCJ

MARCELO VANDRÉ RIBEIRO BARRETO FILHO

OS CONTORNOS JURÍDICOS DA LEI GERAL DE PROTEÇÃO DE DADOS FRENTE AO CONSUMO NO AMBIENTE VIRTUAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro de Ciências Jurídicas da Universidade Federal da Paraíba, como exigência parcial da obtenção do Título de Bacharel em Ciências Jurídicas.

Aprovado em: Santa Rita-PB, 20 de setembro de 2019.

BANCA EXAMINADORA

_____

Prof. MS. Alex Taveira dos Santos
Orientador

_____

Prof. Dr. Gustavo Rabay Guerra

_____

Prof. Dr. Romulo Rhemo Palitot Braga

AGRADECIMENTOS

Uma nova jornada, um ciclo se encerra e outro se inicia. Há cinco anos dei início a este sonho, hoje estou encerrando uma etapa vitoriosa, cheia de desafios e descobertas, na qual eu pude me reinventar e atestar minha capacidade para os novos desafios que estão por vir.

Agradeço primeiramente ao meu bom Deus pelo dom da vida e pelas graças alcançadas.

Aos meus pais, meu total sentimento de gratidão. Todo amor, dedicação, investimento e educação que recebo desde o meu nascimento forjaram a minha personalidade e me faz lutar por objetivos cada vez mais altos. Obrigado por me ensinarem a caminhar e assim poder seguir meus próprios passos.

Aos meus avós, irmãos, primos, tias, tios, namorada e amigos, meu sentimento de gratidão ao que representam na minha formação como homem, Deus foi muito generoso ao me colocar perto de pessoas como vocês, carrego no meu coração todo bom momento vivido ao lado de cada um, muito obrigado por tudo.

Ao meu orientador, Alex Taveira, minha gratidão por todos esses anos de amizade e ensinamentos durante o curso, sendo um dos exemplos de homem que carrego para minha vida.

Por fim, agradeço a oportunidade em trabalhar com grandes profissionais que me inspiram na advocacia, obrigado pela paciência e ensinamentos passados, vocês foram essenciais nessa caminhada. Assim, represento todos os colegas de trabalho nas pessoas de Marina Lacerda Cunha Lima, Icaro Rebouças Marcelino, Romulo Rhemo Palitot Braga e Gustavo Rabay Guerra.

RESUMO

A nova era digital e as mudanças socioeconômicas causadas pela internet ensejaram o início de novas relações jurídicas, assim, o presente trabalho tem como objetivo avaliar os contornos jurídicos da Lei Geral de Proteção de Dados – Lei nº 13.709/18 – a qual fora publicada em agosto de 2018 e encontra-se em *vacatio legis* até agosto de 2020. Inspirada na legislação Europeia e acompanhando os avanços legislativos mundiais acerca do tema, a lei dá nova ideia à proteção de dados pessoais no Brasil, assegurando ao titular dos dados um maior controle acerca das suas informações, baseada em diversos princípios como o da privacidade e o da intimidade. Assim, busca uma melhor análise sobre a forma a qual a referida lei irá diminuir as violações sofridas pelos consumidores no âmbito virtual, bem como a necessidade de as empresas estarem em conformidade com o novo regramento.

Palavras-chave: Lei Geral de Proteção de Dados; Dados Pessoais; Consumidor; Internet; Direito Digital.

ABSTRACT

The new digital age and the socioeconomic changes caused by the internet have led to the beginning of new legal relationships. Thus, this paper aims to evaluate the legal contours of the General Data Protection Law - Law No. 13.709 / 18 - which was published in August 2018 and is in vacatio legis until August 2020. Inspired by European legislation and following the worldwide legislative advances on the subject, the law gives new idea to the protection of personal data in Brazil, ensuring the data subject greater control. about your information, based on several principles such as privacy and intimacy. Thus, it seeks a better analysis of how this law will reduce the violations suffered by consumers in the virtual scope, as well as the need for companies to comply with the new rule.

Keywords: Law of protection data; Personal data; Consumer; Internet; Digital law.

SUMÁRIO

1. INTRODUÇÃO

A presente monografia tem como metodologia a pesquisa do tipo bibliográfica, buscando suas referências através da análise da literatura já publicada em forma de livros, artigos, periódicos, bem como busca um maior esclarecimento através de casos práticos. O método de pesquisa utilizado é o dedutivo, haja vista que as conclusões são realizadas através de análise de informações.

O trabalho tem por tema uma análise dos contornos jurídicos da Lei nº 13.709/18 – Lei Geral de Proteção de Dados – em face dos consumidores no âmbito virtual, avaliando todos os momentos históricos antes da lei e sua severa importância ao instituto da proteção de dados pessoais, acompanhando a evolução da legislação mundial.

Inicialmente, o capítulo 2 irá ater-se ao consumidor no ambiente virtual, avaliando que a sociedade de consumo da maneira que se encontra é fruto da globalização e a forte influência da internet.

A qual nasce a partir do advento da Sociedade de Informação ou Sociedade Pós-Industrial, devido ao grande avanço tecnológico e a característica do hiperconsumo, mudando todas as relações sociais e econômicas existentes, para tanto, utiliza-se o importante conceito de Amadeu da Silveira:

> As sociedades informacionais são sociedades pós-industriais que tem a economia fortemente baseada em tecnologias que tratam informações como seu principal produto. Portanto, os grandes valores gerados nessa economia não se originam principalmente na indústria de bens materiais, mas na produção de bens imateriais, aqueles que podem ser transferidos por redes digitais. Também é possível constatar que as sociedades informacionais se estruturam a partir de tecnologias cibernéticas, ou seja, tecnologias de informação e de controle, as quais apresentam consequências sociais bem distintas das tecnologias analógicas, tipicamente industriais. (SILVEIRA, 2017, p. 13 e 14)

Assim, a valorização da informação, tecnologia e conhecimento são fundamentais para entendermos a sociedade de consumo a qual estamos inseridos, tendo em vista que as empresas passam a se organizar em redes e a valorizar a mão de obra qualificada, dotada de conhecimento técnico específico.

Deste modo, demonstra-se que o conhecimento é cada vez mais disseminado de forma rápida, principalmente através da rede mundial de computadores, os quais

possibilita a troca instantânea de informações, concretizando um novo modelo de sociedade baseada na tecnologia.

Em seguimento, uma analisada pormenorizada acerca do comércio eletrônico e a sua ascensão devido ao acesso à internet é realizada, citando os principais benefícios desta nova sociedade de consumo pautada pelos meios digitais, salientando a redução de custos e menos tempo gasto como os principais benefícios, no entanto, ressalta a grande possibilidade de cometimento de irregularidades, as quais vão desde fraudes à venda de dados pessoais.

Prosseguindo, irá o capítulo 3 versar acerca da fragilidade da segurança digital do consumidor, analisando as nuances dos meios eletrônicos, bem como sua facilidade em cometer delitos, citando estudos de casos para comprovar tal tese e o combate da legislação acerca do tema.

Preocupando-se principalmente com os crescentes casos de vazamento de dados pessoais, o referido capítulo analisa a ação dos *hackers* e a consequente falta de segurança por parte das empresas detentora dos dados ou até mesmo de boa-fé, tendo em vista que muitos dados são coletados e autorizados pelos usuários, através do contrato de adesão em letras miúdas, a serem utilizados com fins diversos, chegando até mesmo a ocorrer a mercantilização desses dados.

Assim, o direito fundamental à privacidade não está sendo cumprido e os grandes casos de vazamento de dados demonstram isso, no entanto, ressalta-se a evolução legislativa citando-se principalmente o Regulamento Geral de Proteção de Dados na União Europeia e a Lei Geral de Proteção de Dados na jurisdição brasileira.

Desta maneira, as informações inseridas no meio virtual tornam-se uma moeda valiosa nos tempos atuais, sendo chamada por alguns de “ouro virtual” devido ao seu alto valor e importância, principalmente quando o assunto é a chamada publicidade direcionada.

A referida publicidade consiste em um cruzamento de informações a fim de gerar perfis personalíssimos, portanto, simples buscas na internet já demonstram seu perfil de consumidor e esse dado é compartilhado com as empresas fornecedoras dos serviços.

O autor Bruno Ricardo Bioni, 2019, p.18, faz uma importante abordagem acerca do acúmulo de dados para direcionamento da publicidade.

> Diversos outros serviços utilizam da mesma técnica, catalogando o comportamento do usuário para, a partir daí direcionar uma publicidade condizente ao seu perfil inferido. O usuário da rede é, portanto, a todo momento, monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária. (BIONI, 2019, p. 18)

Desta forma, percebe-se que a sociedade atual é pautada pelo controle e qualidade dos dados acumulados, no entanto, crescentes são as atuações criminosas que mercantilizam os referidos dados ou os utiliza para crimes mais específicos.

Dando seguimento, o presente capítulo irá fazer uma importantíssima análise acerca dos vazamentos de dados e os métodos de segurança, exemplificando através dos casos do Facebook, Uber e Faceapp.

Demonstrando a necessidade de maiores investimentos na segurança dos meios virtuais, sendo de suma importância para a reputação e controle da cadeia produtiva das empresas, bem como uma maior transparência na relação com seus consumidores.

O capítulo 4 analisa a importante evolução legislativa acerca da proteção de dados no Brasil, chegando ao patamar que estamos com a Lei geral de Proteção de Dados.

Inicialmente, dispõe acerca do remédio constitucional do Habeas Datas, disposto no art. 5º, LXXII da nossa Carta Magna, responsável por ensejar a proteção aos dados pessoais como direito fundamental, dando início à nova era de informação no ordenamento jurídico brasileiro.

Em seguida, demonstra o advento do Código de Defesa do Consumidor como sendo de suma importância para garantir a privacidade dos seus consumidores, analisando que o art. 43 da referida lei dispõe acerca do direito do consumidor ao acesso às informações existentes, bem como os seus dados pessoais e de consumo.

Prosseguindo, relata o advento do novo Código Civil Brasileiro como de grande valia, tendo em vista que dedica capítulo próprio à proteção da vida privada e personalidade dos indivíduos, com isso, aliado ao Código de Defesa do Consumidor, torna-se importante instrumento de preservação da privacidade e personalidade dos indivíduos.

A Lei de Acesso à Informação é tratada como a primeira lei federal recepcionada no contexto da internet, sua importância deriva do fato de trazer noções introdutórias mais específicas acerca da proteção de dados, conceituando o que seria

“informação”, no entanto, é restrita ao submeter apenas os entes da administração pública direta e indireta.

Como a última lei analisada antes do contexto da Lei Geral de Proteção de Dados surge o Marco Civil da Internet, o qual regula as condições e uso da internet, dispondo de responsabilização civil para irregularidades e privilegiando os direitos fundamentais à dignidade e privacidade.

Assim, o Marco Civil dá início à nova era da proteção de dados no Brasil, no entanto, a proteção de dados ainda carece de legislação específica, assim, em 2018, publica-se a Lei º 13.709/18 – Lei Geral de Proteção de Dados.

Desta forma, o capítulo 5 da presente monografia irá fazer uma análise pormenorizada acerca da Lei º 13.709/18, a qual encontra-se em *vacatio legis* até agosto de 2020, representando uma grande conquista do ordenamento jurídico brasileiro, acompanhando a evolução legislativa mundial acerca da temática.

O Artigo 5º da presente lei traz diversos conceitos que precisarão ser compreendidos para uma boa aplicação da norma, bem como demonstra intenção da lei em proteger a pessoa natural titular de dados pessoais.

Assim, a referida lei dá total controle ao titular dos dados acerca da utilização, coleta e tratamento dos dados obtidos, permitindo uma maior transparência entre o titular e o fornecedor.

Em seguimento, realiza-se uma importantíssima análise em cada princípio disposto no artigo 6º da presente lei, a fim de entendermos a importância e capacidade da Lei Geral de Proteção de Dados.

O tópico 5.2 é de suma importância para o desfecho da temática, tendo em vista que trata acerca da responsabilidade civil no âmbito da proteção de dados, gerando o dever das empresas em reparar os danos cometidos, ressaltando-se que trata de uma responsabilidade objetiva.

No seu próximo tópico, analisa-se a importância das empresas estarem em conformidade com a citada lei, sob pena de responsabilização pelos danos decorrentes e uma série de danos à imagem da empresa, desta forma, deverá haver uma maior atenção das empresas com o tema, alterando suas políticas de segurança e seu código de conduta ética.

Por fim, o presente trabalho discorre acerca da viabilidade da Lei geral de Proteção de Dados como forma de inibir as violações sofridas pelos consumidores, sendo esta uma grande ferramenta que, mesmo ainda não sendo aplicada no nosso

ordenamento jurídico, já podemos esperar grandes conquistas, tendo em vista a mudança de patamar da proteção aos dados pessoais dada pela legislação análoga, qual seja o Regramento Geral de Proteção de Dados da União Europeia, a qual serviu de espelho para a Lei nº 13.709/18 – Lei geral de Proteção de Dados.

2. O CONSUMIDOR NO AMBIENTE VIRTUAL

A sociedade de consumo nos moldes que se encontra nos idos atuais, com forte influência da internet, é fruto da globalização que fora capaz de transformar não somente as relações de consumo, mas também as relações sociais e culturais estabelecidas entre os indivíduos.

Deste modo, para compreensão de tal transformação, é imprescindível a utilização do arcabouço histórico, tendo em vista que a partir do século XVIII, com o início da primeira fase da Revolução Industrial, o consumo toma novas formas, passando a ser desempenhado por novos grupos e sob novas influências, introduzindo-se nas diversas camadas da sociedade.

No entanto, apenas ao fim do século XX, tem início a chamada sociedade de informação, a qual possui como característica o hiperconsumo atrelado ao grande avanço tecnológico e significativa diversidade de meios de comunicação decorrentes do uso da internet pelos diversos setores da sociedade e da economia, ensejando em novas relações de consumo pautadas pelos meios eletrônicos.

2.1 A sociedade de informação

A revolução da tecnologia da informação e a sociedade pós-industrial formam a base histórica da chamada sociedade de informação, sendo este conceito derivado de uma combinação de elementos que ensejam uma nova relação socioeconômica.

A internet, televisão e telefonia são os grandes elementos desta nova sociedade, gerando a consequente desmaterialização dos espações produtivos. Ou seja, a sociedade de informação é na essência computacional e informática.

Neste sentido, bem preceitua Maria Julia Giannasi, 1999:

> A definição mais comum de Sociedade da Informação enfatiza as inovações tecnológicas. A ideia-chave é que os avanços no processamento, recuperação e transmissão da informação permitiram aplicação das tecnologias de informação em todos os cantos da sociedade, devido a redução dos custos dos computadores, seu aumento prodigioso de capacidade de memória, e sua aplicação em todo e qualquer lugar, a partir da convergência e imbricação da computação e das telecomunicações (GIANNASI, 1999, p.21).

Depreende-se que nesta sociedade de informação a relações estão centradas nos serviços e principalmente no conhecimento técnico, a qual possui grande valia neste novo contexto de organização social.

Trata-se de uma nova etapa no desenvolvimento da sociedade, caracterizada pelo crescente papel da informação nas novas relações, rompendo barreiras geográficas com a formação de um novo espaço global de trocas de conhecimento.

Daniel Bell, 1973, em sua obra: “O advento da sociedade de informação”, explana que a sociedade pós-industrial deve ser analisada a partir de cinco dimensões, sendo estas dimensões geradoras de transformações severas na sociedade.

Perpassando por todas as dimensões, devemos nos ater principalmente à quinta e última dimensão, a qual deve ser compreendida a partir do “aparecimento de uma nova tecnologia intelectual, ou seja, criação de regras para soluções de problemas incorporadas a uma máquina automática ou a um programa de computador, que resulta na ascensão de novas elites técnicas.” (BELL, 1973, p. 27).

Daniel Bell, 1973, em busca do conceito de sociedade pós-industrial, já passa a discutir o surgimento da expressão “Sociedade de Informação”, tendo em vista a correlação dessa nova fase da sociedade com a importância da informação em setores da economia e política da sociedade, refletindo, desta maneira, na organização cultural dos indivíduos.

Acerca do conceito de sociedade informacional, podemos citar Sérgio Amadeu da Silveira, 2017:

> As sociedades informacionais são sociedades pós-industriais que tem a economia fortemente baseada em tecnologias que tratam informações como seu principal produto. Portanto, os grandes valores gerados nessa economia não se originam principalmente na indústria de bens materiais, mas na produção de bens imateriais, aqueles que podem ser transferidos por redes digitais. Também é possível constatar que as sociedades informacionais se estruturam a partir de tecnologias cibernéticas, ou seja, tecnologias de informação e de controle, as quais apresentam consequências sociais bem distintas das tecnologias analógicas, tipicamente industriais. (SILVEIRA, 2017, p. 13 e 14)

No campo econômico, observa-se a informação como fator primordial para o desenvolvimento dos novos moldes do capitalismo, caracterizado, principalmente, pela descentralização das empresas, organizando-se em redes e pela valorização da mão de obra qualificada, dotada de conhecimento.

A tecnologia e o conhecimento ganham ênfase nesta etapa pós-industrial haja vista a concorrência global e a necessidade de redução do preço final dos produtos, devendo, desta forma, haver uma redução na mão de obra desqualificada, e maior inserção da tecnologia no sistema produtivo.

Desta forma, há de se falar que a informação possui elevado valor nessa sociedade pós-industrial, tendo em vista a maior produção baseada na técnica e no conhecimento. Assim, a tecnologia aliada ao conhecimento domina este novo modelo de sociedade.

No mesmo sentido, a informação globalizada e universal, expandida através de uma rede de computadores, dita os novos rumos da sociedade pós-industrial, haja vista a criação de novos canais de interação entre os indivíduos, disseminando de forma cada vez mais rápida o conhecimento, moldando a vida de todos os indivíduos nela inseridos.

Desta maneira, é nítido que as tecnologias de informação ditaram os novos padrões da economia global, concretizando um novo modo de produção e comunicação da sociedade, algo que ao longo do tempo irá se aprofundar cada vez mais com o advento da internet e a criação de tecnologias cada vez mais capazes de suprir todas as necessidades da sociedade, principalmente nas relações de consumo.

Assim, o desenvolvimento das novas tecnologias de informação propiciou uma enorme troca de dados entre os indivíduos espalhados pelo mundo, tal revolução tecnológica dar-se início à chamada sociedade de informação, a qual consiste na globalização desta troca de informações, permitindo uma maior interação entre os seres dos diversos Países.

Desta forma, o surgimento da sociedade de informação transforma-se em um fenômeno que representa uma severa mudança na organização da economia e da sociedade, tendo em vista que as estruturas passam a ser organizadas através, principalmente, da internet.

As transformações causadas pela internet impactaram fortemente a sociedade, na qual é possível realizar quase todas as tarefas e obrigações diárias com o auxílio de um meio eletrônico, dando ensejo a um mundo virtual que funciona em harmonia com o mundo real.

Ademais, imperioso destacar que na era digital, período em que vivemos, a internet não se limita tão somente ao uso de computadores, destaca-se a inclusão de relógios, celulares, televisores, carros, ou seja, nota-se que é quase impossível um

indivíduo estar inserido na sociedade sem uso desta importante ferramenta, destacando a sua dependência nos diversos setores sociais e econômicos.

Com isso, este novo cenário socioeconômico pautado pela Internet acarreta novas relações de consumo, transformando e incentivando a comercialização de bens e serviços de forma cada vez mais rápida e interativa, passando a ser um novo e crescente espaço de comércio.

2.2 Ascensão da internet e o comércio eletrônico

Vivemos hoje em um período pós-modernidade, na qual as relações foram totalmente mudadas com o advento da internet, possibilitando uma comunicação instantânea com todo o planeta, bem como manter relações comerciais, tudo através de equipamentos tecnológicos que se desenvolvem cada vez mais.

O acesso à Internet fora massificado em decorrência do barateamento de produtos que permitem o acesso e o notável desenvolvimento tecnológico ocorrido no século XX, com o início da sociedade de informação.

Assim, a internet difundiu-se ao ponto de quase todas as relações comerciais e sociais serem pautadas através desta, seja uma simples conversa com outros indivíduos de qualquer parte do mundo ou o próprio comércio eletrônico, derivando novas situações jurídicas que o ordenamento jurídico precisou abarcar.

O conceito de Internet está bem explanado na Lei 12.965/14 (Marco Civil da Internet), que em seu artigo 5º, I diz que:

> Art. 5º Para os efeitos desta Lei, considera-se:
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; (BRASIL, 2014)

A internet e as consequentes facilidades de comunicação impactaram os negócios jurídicos, acarretando no surgimento do comércio eletrônico, desta forma, as relações comerciais que até então eram realizadas apenas presencialmente passaram a ter novos moldes.

A ascensão meteórica deste tipo de comércio é explicada através das facilidades encontradas pelo consumidor e pelos fornecedores, tendo em vista que os

produtos podem ser comercializados em qualquer parte do mundo de forma rápida e prática, sem a necessidade da presença física das partes.

Claudia Lima Marques, na sua obra Confiança no comércio eletrônico e a proteção do consumidor, explana o conceito de mercado eletrônico sob dois aspectos:

> Podemos definir comercio eletrônico de uma maneira estrita, como sendo uma das modalidades de contratação não presencial ou à distância para a aquisição de produtos e serviços através do meio eletrônico ou via eletrônica. De maneira ampla, podemos visualizar o comércio eletrônico como um novo método de fazer negócios através de sistemas de redes eletrônicas. (MARQUES, 2004, p. 38)

Portanto, compreende-se o comércio eletrônico como um negócio jurídico realizado através do ambiente virtual, sem qualquer contato físico entre as partes, eliminando as barreiras geográficas e diminuindo os custos das transações.

Essa nova era digital, em que as relações de consumo foram totalmente remodeladas trouxe consigo consideráveis benefícios ao desenvolvimento da sociedade, no entanto, também há de se considerar a necessidade uma maior proteção ao usuário destes serviços, o que será mais bem explorado em tópico próprio.

Não restam dúvidas que o principal benefício do comércio eletrônico está na melhoria da relação entre consumidor e fornecedor, uma vez que há um menor custo para inserção dos produtos no ambiente virtual, permitindo uma maior eficiência nessa relação de compra e venda.

Tal redução de custo pode ser compreendida em razão da redução da mão de obra, desnecessidade de espaço físico, utilidade da internet como domínio público, publicidade menos onerosa, entre diversos fatores que tornam esta nova modalidade de comércio como basilar para a sociedade moderna.

Ademais, ao consumidor coube a vantagem de realizar uma maior pesquisa dos produtos procurados, tendo a possibilidade de escolha com menos tempo gasto do que o necessário para caso este processo fosse feito fisicamente. Com o ambiente virtual funcionando de forma instantânea, o consumidor pôde economizar tempo e reduzir custos, algo extremamente buscado pelo homem moderno.

Aos fornecedores coube a oportunidade de realização de um *marketing* direcionado aos diversos públicos, incentivando cada vez mais o hiperconsumo e aumentando significativamente a venda de seus produtos ou serviços ofertados.

O comércio eletrônico ainda trouxe consigo a oportunidade dada a produtos menos expressivos, com sua marca pouco divulgada, pois, diante da redução de custos e facilidades encontradas no âmbito virtual, essas marcas puderam ter a visibilidade que em meio físico não seria possível, ocorrendo uma democratização da concorrência, monopolizada até então pelos grandes fornecedores com maior poder aquisitivo.

Há de se ressaltar também a inserção de novos modelos de trabalho surgidos com o advento do comércio eletrônico, exemplo do chamado *market place,* o qual consiste em empresas que disponibilizam seu espaço de vendas e publicidade para que outras empresas possam vender seus produtos, funcionando apenas como intermediários por deterem conhecimento acerca do assunto e grande visibilidade são exemplos de grandes empresas virtuais que participam deste mercado: Americanas, Shoptime, Walmart, Mercado Livre e OLX.

Laura de Toledo Ponzoni Marcondes, em sua obra: “Aplicação do código de defesa do consumidor ao comércio eletrônico” cita os atrativos desta nova modalidade de comércio, vejamos:

> Muitos são os atrativos do comércio eletrônico. Ele permite a concretização dos negócios de maneira mais célere; é inegavelmente mais cômodo, já que o consumidor pode realizar negócios diretamente de sua residência, ou do local que mais lhe aprouver; facilita o acesso a mais opções, a coleta de informações e a realização de pesquisas sobre os produtos ou serviços a serem adquiridos; e, e alguns casos, são ofertados preços menores que os praticados nos estabelecimento empresariais dos fornecedores, já que ocorre a redução dos custos operacionais. (MARCONDES, 2013, p. 411)

No entanto, em que pese haver grandes benefícios, os negócios jurídicos realizados através do comércio eletrônico necessitam ainda de grande cautela por parte daqueles que fazem uso, tendo em vista que as facilidades trazidas para o desenvolvimento comercial também podem ser usadas para cometimento de irregularidades, que vão desde fraudes à venda de dados pessoais.

Os dados inseridos pelos usuários no âmbito virtual, sejam eles em plataformas pagas ou aplicativos gratuitos, são utilizados por empresas a fim de direcionar ofertas, violando o direito à privacidade e intimidade destes usuários.

Desta forma, inúmeros são os abusos sofridos pelos consumidores por meios eletrônicos, haja vista a utilização não autorizada dos dados fornecidos a outras empresas e contratos realizados sem autonomia da vontade, havendo uma quebra na

relação de confiança entre os consumidores e fornecedores, que até então só traria benefícios.

Em regra, os negócios jurídicos celebrados presencialmente possuem autonomia da vontade, o que não ocorre no âmbito virtual, sendo este um contrato de adesão sem negociação de cláusulas entre as partes, com o consumidor hipossuficiente nesta relação e com a necessidade de ser tutelado.

Eurípedes Brito Cunha Júnior esclarece o que vem a ser contrato eletrônico, subdividindo-o, vejamos:

> O contrato celebrado mediante meios eletrônicos, ou seja, eletrônico na sua formação, pode ser considerado mais eletrônico do que um contrato avençado por modo tradicional, mas com execução eletrônica. Assim, pode afirmar que o contrato celebrado eletronicamente é eletrônico stricto sensu, enquanto o contrato simplesmente executado eletronicamente é latu sensu. Portanto, as duas categorias estão compreendidas dentro do escopo dos contratos eletrônicos. (CUNHA JÚNIOR, 2002, p. 68).

Dito isto, é importante ressaltar que o contrato eletrônico não difere sua natureza jurídica dos contratos já conhecidos, pois apenas o meio de celebração ou execução que difere, submetendo-se as mesmas regras jurídicas dos realizados presencialmente.

Assim, nota-se a fragilidade ainda existente no âmbito virtual, em que pese ser um contrato como outro qualquer, o fato de ser realizado por meio de uma cadeia de computadores interligados aumenta os riscos à segurança deste negócio jurídico.

A segurança neste ambiente virtual vem sendo objeto de amplos debates da sociedade brasileira e pelo mundo. Com a crescente utilização de meios eletrônicos, nasce a necessidade das leis se adequarem ao novo molde da sociedade, desta maneira observa-se a redação de importantes leis como o Marco Civil da Internet e a Lei geral de proteção de dados, que entrará em vigor a partir de agosto de 2020.

O Marco Civil da Internet (Lei 12.965/14) fora fundamental para dar início a essa nova era de tutela jurídica no ambiente virtual, o que até então era ambiente desconhecido para o judiciário brasileiro passa a ter legislação própria que assegura ao usuário uma maior segurança principalmente no que tange à privacidade dos dados ali dispostos, aqui destaco os artigos 7º e 8º desta lei:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> [...]
> 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. 8º 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.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput**,** tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. (BRASIL, 2014)

Ainda assim, mesmo com o considerado avanço do Marco Civil da Internet, o usuário de meios eletrônicos terá uma nova ferramenta de proteção ao seu dispor, trata-se da Lei Geral de proteção de dados (Lei 13.709/18) que entrará em vigor em agosto de 2020, contemplando um grande avanço na segurança jurídica das informações disponibilizadas pelos consumidores eletrônicos, assegurando o direito à privacidade ao cidadão, preceito fundamental disposto em nossa constituição federal.

Observa-se em sua redação:

> 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)

Assim, confirma-se que a tutela jurídica dos negócios realizados por meios eletrônicos vem ganhando significativa importância no nosso ordenamento jurídico, o que até então era ambiente livre passa a ter leis que o regulamenta.

No mesmo sentido, o Direito deverá evoluir em conjunto com a sociedade, a fim de garantir a ordem e assegurar as prerrogativas fundamentais dos indivíduos inseridos no meio eletrônico, portanto, diante da evolução da sociedade para era digital, nasce o Direito Digital, tendo fundamental papel na nova organização social.

Ainda com os mecanismos da lei ao seu favor, os consumidores sofrem violações diárias, seja na hora de compras eletrônicas ou na utilização de aplicativos

gratuitos, sendo a internet um campo de difícil controle e com enorme crescimento, devendo este trabalho ater-se a tais violações e a forma a qual a nossa legislação enfrenta essa insegurança, principalmente com o advento da Lei geral de Proteção de Dados.

3. A FRAGILIDADE DA SEGURANÇA DIGITAL DO CONSUMIDOR

A revolução causada pela internet, em que as relações sociais, econômicas e culturais são pautadas através desta, trouxe sérias dúvidas quanto à segurança deste meio, levando a sociedade a discutir acerca do uso seguro e consciente da internet.

Além de preocupar-se com fraudes e golpes, os crescentes casos de vazamento de dados pessoais sensíveis levaram os usuários a questionarem cada vez mais os riscos deste meio virtual, aqui citamos casos icônicos das empresas Uber e Facebook, as quais terão maior explicação em tópico próprio.

Entre as diversas formas de inserção do indivíduo no mundo virtual, maior parte delas faz uso dos dados pessoais dos usuários, no entanto, nem sempre essas informações são utilizadas de boa-fé, sem qualquer abuso ou ato ilícito.

Seja em ataques criminosos de *hackers* ou até mesmo venda de dados por parte das empresas que os detém, fato é que os usuários não possuem pleno acesso e conhecimento aos termos e condições em que as empresas coletam e armazenam seus dados, transmitindo-os à terceiros sem o seu consentimento e, para grande parte da população, sem o conhecimento técnico necessário para discernir acerca da gravidade deste fato.

A preocupação legislativa que o Brasil e principalmente a Europa vem dando ao tema da proteção de dados pessoais decorre do preceito fundamental do direito à privacidade, a qual teve sua concepção remodelada na nova sociedade de informação.

Essa fragilização da privacidade decorre do caráter aberto e impessoal que a internet possui, momento em que há uma quebra de barreiras geográficas e interliga uma gigantesca rede de computadores tais dados ficam expostos e sua violação facilitada. Ressaltando-se ainda que essa violação à privacidade do indivíduo não decorre mais tão somente da exposição da sua vida íntima, algo mais pensado no contexto anterior à sociedade de informação.

Laura Schertel Mendes, em sua obra: “O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor”, bem referencia a necessidade do consumidor em ter o direito ao controle dos seus dados pessoais, bem como a garantia ao consumidor da forma a qual será utilizado.

> (i) a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação

> dos dados pessoais e (ii) a atribuição ao consumidor da garantia de controlar o fluxo de seus dados na sociedade. (MENDES, 2016, p. 44)

Assim, não estamos inseridos em um momento histórico em que a privacidade é regra, e sim a exceção, os crescentes casos de vazamento e tratamento irregulares aos dados demonstram isso. Desta forma, há a necessidade de as empresas estarem em conformidade com a nova era da sociedade digital, a qual há uma preocupação de sobremaneira com as regras de segurança da informação, citando como exemplo o Regulamento Geral de Proteção de Dados na União Europeia e a Lei Geral de Proteção de Dados na jurisdição brasileira.

Desta maneira, uma análise acerca dos riscos enfrentados pelos usuários de plataforma digitais se faz necessária, bem como uma eficaz legislação e fiscalização acerca do correto tratamento aos dados pessoais sensíveis dos indivíduos, assegurando ao consumidor/usuário uma total segurança e controle dos seus dados disponibilizados, no entanto os crescentes casos de grandes empresas envolvidas em escândalos de vazamento de dados põem cada vez mais em dúvida a segurança dos meios eletrônicos.

3.1 Violação à proteção de dados pessoais e as ilegalidades cometidas

As relações de consumo sofreram significativas mudanças com o advento da Internet, desta forma, a concorrência comercial ganhou novos moldes, tendo a publicidade ganhado maior importância, haja vista a possibilidade instantânea comunicação e o rompimento de barreiras geográficas, ocasionando em um maior público atingido em menos tempo e de forma bem menos onerosa do que a convencional.

Desta forma, essa transformação nas relações comerciais trouxe consigo uma grande busca pelo direcionamento da publicidade, assim, as informações inseridas pelos usuários nos meios eletrônicos tornam-se uma moeda valiosa nos tempos modernos.

Simples buscas na internet por determinados produtos são capazes de criar perfis personalíssimos dos usuários, algo explorado economicamente pelas empresas detentoras desses dados e que possuem espaços de publicidade nas suas páginas eletrônicas, desta maneira, há uma compartilhamento com as empresas fornecedoras

dos produtos, as quais são capazes de direcionar a publicidade àquele perfil de usuário, aumentando assim sua chance de compra.

Tal prática é denominada de publicidade direcionada, a qual consiste em um cruzamento de informações a fim de gerar perfis personalíssimos dos usuários. Estes dados são cada vez mais armazenados e submetidos a um processo de organização e filtro, gerando um perfil completo do consumidor, sendo possível saber suas preferências e necessidades de forma instantânea.

O autor Bruno Ricardo Bioni, 2019, p.18, faz uma importante abordagem acerca do acúmulo de dados para direcionamento da publicidade.

> Diversos outros serviços utilizam da mesma técnica, catalogando o comportamento do usuário para, a partir daí, direcionar uma publicidade condizente ao seu perfil inferido. O usuário da rede é, portanto, a todo momento, monitorado, acumulando-se uma série de dados (comportamentais), que são aplicados para a personalização da abordagem publicitária. (BIONI, 2019, p. 18)

Segundo Mendes (2016, p.51) essa prática consiste em discriminação ao consumidor, vez que o armazenamento de dados pessoais do consumidor para fins de criação de perfis personalíssimos, oferecendo tratamento de preços e ofertas específicas para os usuários que se encaixam no perfil vantajoso ao fornecedor, acarreta em violação ao princípio da igualdade disposto na Constituição Federal e no Código de Defesa do consumidor, ainda cita a autora que esta forma de tratamento de dados, gerando a consequente publicidade direcionada, fere diretamente as normas consumeristas que nos regem.

Outro ponto importante a ser analisado refere-se à coleta de dados no momento do cadastro de usuários, tendo em vista que irá alimentar o banco de dados do fornecedor seja a compra realizada ou não, tal fato implica tanto na publicidade direcionada quanto na fidelização do cliente.

Acerca da segurança em face dessa grande massa de dados armazenados, Liliana Minardi Paesani, 2003, bem preceitua:

> A Internet insere-se em contexto permeado de paradoxos: trata-se da mídia que conta com mais meios de proteção de privacidade e integridade (relembre-se aqui a figura das senhas, da criptografia, da biométrica etc.), porém é a mais suscetível a ataques e invasões (como os desfechados pelos hackers e crackers, em relação a sistemas tidos como seguros), bem como a outros tipos de danos como os causados por vírus. Da mesma forma, é a indústria do desenvolvimento mais caro e especializado, porém é a que oferece literatura técnica mais farta e acessível. (PAESANI, 2013, p. 67-68)

Nota-se que a sociedade atual baseia-se no controle de informações, em que relações sociais e econômicas estão sendo pautadas pela quantidade e qualidade dos dados coletados, no entanto, tal coleta de dados gera uma enorme preocupação no que tange à segurança deste meio, haja vista as crescentes atuações criminosas causadas por *hackers* bem como a venda de dados para fins de publicidade direcionada.

Ademais, devemos entender consumidor no sentindo amplo da palavra, aqui enquadramos como consumidor também o usuário de plataformas gratuitas, que vão desde redes sociais à aplicativos de entretenimento, sendo esta classe a principal responsável pela grande massa de coleta e armazenamento de dados.

A maioria destes aplicativos e redes sociais solicitam mais informações que o necessário para a prestação do serviço, apesar de quase sempre dispor nas miúdas letras da política de privacidade, não é comum aos usuários atentarem-se às especificações e permissões ali contidas quando do aceite, abastecendo este banco de dados sem saber qual será a destinação dada.

Assim, a preocupação pelo armazenamento dos dados pessoais coletados pelas empresas cresce no sentido que a atuação desses *hackers* se profissionaliza cada vez mais, bem como aumenta a cobrança da sociedade e do judiciário para que tais empresas ofereçam maior segurança aos seus clientes/usuários.

O advento de leis que regulam o tratamento aos dados pessoais, a exemplo da legislação da União Europeia e Brasileira, firma uma conscientização da necessidade de aumentar a segurança nos meios virtuais, grandes empresas somam grandes altas montas em multas decorrentes de vazamentos de dados, colocando em xeque sua reputação e arranhando sua imagem comercialmente.

No mesmo sentido, Patricia Peck Pinheiro, 2011, bem preceitua essa relação das empresas em face de sua reputação no que tange à proteção de dados:

> A maioria das empresas virtuais que sofrem invasões não denuncia a ocorrência, haja vista que os dados furtados são de seus ‘clientes’ e muitas vezes serão utilizados por terceiros sem que estes percebam, pelo menos até que algo pior ocorra (...). Alguns têm medo de tornar a ocorrência pública por temerem que haja dano à marca, que passaria a imagem de ser insegura perante o universo dos consumidores. (PINHEIRO, 2011, p. 187).

Com isso, nota-se uma tendência das empresas virtuais em tentar camuflar os vazamentos de dados ocorridos, haja vista as consequências da quebra de confiança no consumidor causada, ocasionando, assim, em perda de valor de mercado e grandes prejuízos comerciais para além da multa a ser aplicada em decorrência da falha de segurança.

Portanto, diante desta prática das empresas, é possível que haja mais casos de vazamento ilegal de dados do que os já divulgados, gerando maior insegurança no consumidor em relação ao serviço virtual, ademais, há de se ressaltar a reponsabilidade civil do fornecedor em face das ilegalidades cometidas frente ao consumidor no âmbito virtual, principalmente no que tange ao vazamento de dados.

3.2 Cibersegurança e vazamento de dados

O vazamento de dados pessoais sensíveis dos usuários de meios eletrônicos tornou-se uma das maiores preocupações do homem moderno, tendo em vista as grandes repercussões de casos envolvendo empresas e o vazamento dos dados dos seus clientes, assim, não seria criterioso afirmar que os dados são a nova moeda do mercado digital, sendo talvez a mais valiosa.

Tratar os dados como uma valiosa moeda decorre da sua importância e valor econômico no meio, seja com seu uso para publicidade direcionada ou até mesmo para influenciar campanhas políticas, notando-se, portanto, a total influência do meio virtual em todos os aspectos do cotidiano do homem contemporâneo.

O vazamento de dados é a falha de segurança que mais deve preocupar o usuário, tendo em vista tratar-se de um acesso indevido com fins ilícitos a provedores e plataformas eletrônicas para roubo de dados pessoais ou em uma mercantilização não autorizada destes dados.

Assim, tais dados são expostos e usados de maneira não autorizada para fins diversos, enquanto o usuário, confiando na segurança da plataforma utilizada, acreditava estar seguro de que as informações ali inseridas não teriam qualquer outro direcionamento.

Sendo assim, a preocupação com a segurança destes dados, seja por empresas ou pelos usuários deu início ao crescente mercado da cibersegurança, tendo em vista que grande parte das informações valiosas dos serviços empresariais

estão armazenadas em rede, havendo um dever de maior proteção e gerando o consequente investimento por parte das empresas neste ramo.

Posto isso, devemos entender o conceito de cibersegurança como sendo o conjunto de estratégias e habilidades para redução de riscos nas operações realizadas através do meio virtual, protegendo os usuários e fornecedores de ataques de *hackers* ou qualquer tipo de outro acesso não autorizado.

Assim, tendo em vista a responsabilidade objetiva do fornecedor com relação ao armazenamento e utilização dos dados pessoais dos seus usuários, estes devem estar em conformidade com os novos padrões, antecipando-se aos riscos e sendo capaz de desenvolver soluções que tragam segurança aos dados armazenados, evitando, assim, multas milionárias e imagem arranhada em decorrência da falta de confiança dos clientes.

Com isso, o investimento na segurança cibernética passa a ser de grande importância para o patrimônio e reputação da empresa, assegurando toda cadeia de produção, haja vista que os incidentes de vazamento de dados repercutem diretamente em toda cadeia produtiva da empresa, seja ela em negócio digital ou não.

No mesmo sentido, para que as empresas possam estar em conformidade, investir em segurança contra-ataques de criminosos não é o único caminho, uma relação mais transparente com os usuários/consumidores passa a ser vital para a proteção de dados pretendida.

Aqui falamos sobre uma atualização da política de privacidade, política de *cookies* e termos de uso, inclusive evitando as recorrentes letras miúdas que os usuários aderem sem ter o total conhecimento, principalmente quando falamos em uma população que em sua maioria tem acesso a meios virtuais mas não possuem o conhecimento técnico suficiente, muitos deles sequer possuem capacidade de leitura.

Portanto, percebe-se que a preocupação com o armazenamento e tratamento dos dados pessoais coletados passa por um maior investimento em cibersegurança, a fim de evitar atuações criminosas, bem como uma maior transparência na relação com o usuário, conscientizando-o da destinação dada às suas informações inseridas, e, principalmente, com o avanço das legislações em todos os Países no tocante à proteção de dados.

Neste sentido, analisaremos os principais casos de vazamento de dados ocorridos por grandes empresas e suas consequências práticas sob a ótica das legislações brasileiras e internacionais que regem o assunto, situação esta que se

tornou corriqueira nos noticiários nos últimos anos, demonstrando a gravidade com a qual o assunto deve ser enfrentado.

3.2.1 Caso facebook

O caso facebook talvez seja o mais emblemático e representativo quanto à importância da proteção e tratamento dos dados fornecidos pelos usuários, tendo em vista que aliou o vazamento ilegal com a consequente utilização para fins políticos, influenciando a eleição presidencial norte americana vencida por Donald Trump.

O presente vazamento deu-se através de um aplicativo chamado "*this is your digital life",* desenvolvido pela Universidade de Cambridge, o qual consistia na realização de testes de personalidade e seu acesso era feito através da conta do facebook, no entanto, o usuário deveria concordar com os termos de uso e condições do aplicativo, estando nesse incluído a autorização para uso dos dados coletados para fins acadêmicos.

Neste sentido, em que pese os usuários terem autorizado o armazenamento e utilização das informações, o aplicativo também foi capaz de coletar dados da rede de amigos dos usuários que fizeram uso da plataforma, atingindo a mais de oitenta e sete milhões de usuários.

Após ter conhecimento acerca da pesquisa, representantes da *Cambridge Analytica* buscaram formar parceria com a Universidade de Cambridge para obter acesso aos dados, o que de pronto fora negado pela instituição de ensino.

Diante da negativa da instituição de ensino, a empresa entrou em contato diretamente com o responsável pelo aplicativo e desembolsou cerca de US$ 800.000,00 (oitocentos mil dólares) para ter acesso a todos os dados coletados pelo seu aplicativo, em clara violação às condições do Facebook, qual seja a coleta dos dados para fins acadêmicos.

Assim, as informações obtidas foram vendidas à *Cambridge Analytica*, empresa de análise de dados que prestou serviços na campanha do Presidente norte americano Donald Trump em 2016, utilizando-se destes dados para criar um sistema capaz de influenciar e direcionar as escolhas dos eleitores nas urnas.

Esse sistema consistia numa catalogação e definição dos perfis dos usuários, direcionando materiais a favor de Donald Trump e contrário ao seu opositor, agindo principalmente em eleitores que ainda estavam em dúvida quanto ao seu voto.

O facebook, à época do fato, permitia que aplicativos externos coletassem dados referentes aos amigos dos usuários, com a justificativa de ser usado apenas para melhoria do aplicativo, proibindo a venda ou uso para propaganda, o que não ocorreu no presente caso.

O caso fora descoberto pelo facebook em meados de 2015, no entanto, a empresa decidiu abafar o caso e não comunicou aos usuários acerca do vazamento ocorrido.

Desta maneira, em 2018 o caso chegou ao conhecimento da mídia e consequente ao grande público afetado, quando um ex-funcionário da *Cambridge Analytica* montou dossiê sobre o uso ilícito de dados e os repassou a um jornalista do famoso periódico *"The New York Times",* bem como às autoridades americanas.

Diante do comprovado uso indevido de dados, o facebook teve sua imagem arranhada, valor de mercado despencando na bolsa de valores e o seu presidente e fundador, Marck Zuckerberg, convocado a dar explicações públicas ao Comitê Judiciário e de Comércio do Senado nos Estados Unidos.

Resultado: a empresa fora multada, por essa e outras violações, em US$ 5.000.000.000,00 bilhões (cinco bilhões de dólares) pelo órgão que regula o comércio nos Estados Unidos, além de ter que estar em conformidade com as normas de segurança digital, principalmente no tocante a coleta e uso dos dados obtidos.

3.2.2 Caso uber

O referido caso é um clássico exemplo do citado no tópico 3.1 deste trabalho, em que as empresas tentam esconder os vazamentos de dados obtidos para que não tenha sua imagem arranhada e a ocorrência de sanção por parte das autoridades competentes.

Assim, em meados de 2016, a uber sofreu um ataque de hackers que acarretou na exposição de informações pessoais de mais de cinquenta e sete milhões de usuários, dentre os quais cento e noventa e seis mil eram brasileiros.

O roubo de dados fora logo descoberto pela empresa, no entanto, como forma de camuflar o caso e não deixar que chegasse ao conhecimento de seus usuários ofereceu US$ 100.000,00 (cem mil de dólares) para que os hackers destruíssem os dados obtidos.

No entanto, em meados de 2017, um novo presidente executivo fora empossado na empresa e, com a proposta de maior transparência para com seus usuários, revelou o ataque criminoso sofrido.

Tal fato fora entendido pelas autoridades nos Estados Unidos como uma afronta às leis daquele País, com violação flagrante à confiança do consumidor, desta forma, os cinquenta estados norte-americanos propuseram ação para investigação e possível sanção ao incidente ocorrido.

Desta forma, as partes transigiram e chegaram ao valor de US$ 148.000.000,00 (cento e quarenta e oito milhões de dólares) a ser pago pela empresa, bem como a necessidade de implementação de um programa de segurança de informação e relatórios trimestrais acerca de incidentes de segurança de dados.

3.2.3 Caso faceapp

Trata-se de aplicativo que, com inteligência artificial, submete fotografias enviadas pelos usuários para que ocorra envelhecimento facial, tal aplicativo virou febre no Brasil e no mundo, no entanto, aqui demonstra-se um legítimo caso em que os usuários não leem as políticas de privacidade do aplicativo e as aceita sem qualquer conhecimento de direcionamento dos dados ali fornecidos.

Assim, nas condições de uso do aplicativo, que possui natureza contratual, contém cláusula que autoriza os dados ali obtidos serem cedidos a terceiros sem qualquer informação acerca do uso que seria dado, fato que deve ter a máxima preocupação da sociedade, principalmente quando falamos de um servidor disposto na Rússia, fora de qualquer alcance das mais severas leis de proteção de dados.

No Brasil, em razão do aplicativo estar fora de alcance da justiça brasileira, o procon do estado de São Paulo notificou a empresa responsável para oferecer explicações acerca da coleta de dados dos usuários, bem como multou a Google e Apple em R$ 17.000.000,00 (dezessete milhões de reais) por desrespeitar o código de defesa do consumidor ao hospedar em suas lojas um aplicativo que não possui políticas de privacidade e termos de uso escritos em português.

Desta forma, vemos a real importância em uma nova educação digital aos usuários de meios virtuais, a coleta de dados e seu uso indiscriminado estão ganhando proporções jamais vista, devendo a população no geral estar cada vez mais consciente do bom uso de aplicativos para que não venha a ser prejudicada no futuro.

No Brasil, a preocupação com a proteção de dados já é uma realidade, a Lei geral de Proteção de Dados, mesmo em *vacatio legis* até agosto de 2020, tem mudado a forma com a qual as empresas e usuários lidam com o tema. A nova sociedade digital já uma realidade e a legislação brasileira tem acompanhado essa evolução, desde o Código de Defesa do Consumidor, passando pelo Marco Civil da Internet e hoje com a Lei Geral de Proteção de Dados inspirada na eficaz legislação Europeia acerca do tema.

4 EVOLUÇÃO LEGISLATIVA BRASILEIRA SOB A PERSPECTIVA DA PROTEÇÃO DE DADOS PESSOAIS

A internet transformou as relações sociais e econômicas estabelecidas pelos indivíduos, assim, houve a necessidade de evolução também por parte da legislação brasileira, para que esta possa abarcar as novas relações jurídicas derivadas deste novo campo.

Neste breve capítulo iremos compreender tal evolução, desde o remédio constitucional do habeas data à Lei 13.709/18 (Lei Geral de Proteção de Dados).

A nossa Constituição Federal data de 1988, anterior a expansão de internet, sendo assim, não fora capaz de abordar temas específicos como a proteção de dados pessoais no campo virtual.

No entanto, dispõe acerca do remédio constitucional do habeas data como direito fundamental, desta maneira, mesmo que sucinto e limitado, enseja a proteção de dados pessoais como direito fundamental, dando início à nova era da informação no ordenamento jurídico brasileiro.

> Art. 5º
> [...]
> LXXII - conceder-se-á habeas data:
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL, 1988)

No decurso do tempo, em 1990, há o importante advento da Lei nº 8.070/90 (Código de Defesa do Consumidor), a qual também demonstra uma preocupação com a privacidade dos consumidores, a exemplo da interpretação do artigo 43, senão vejamos:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. (BRASIL, 1990)

Já em 2002, houve a instituição do novo Código Civil Brasileiro, Lei nº 10.406/02, a qual dedica o capítulo II à proteção da vida privada e personalidade dos indivíduos, permitindo ainda a atuação judicial para tutelar este direito fundamental, conforme observa-se na redação do art. 21:

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma (BRASIL, 2002).

Já em 2011 há o surgimento da primeira lei federal recepcionada no contexto da internet, trata-se da Lei nº 12.527/11 (Lei de Acesso à Informação), tal norma surge para regular o acesso à informação previsto no art. 5º da Carta Magna, trazendo noções introdutórias importantíssimas acerca da proteção aos dados pessoais, momento em que classifica informação como sendo “dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato” (BRASIL, 2011).

Esse aspecto é de suma importância pois já demonstra um avanço, mesmo que tardio, na preocupação do nosso ordenamento jurídico em proteger os dados pessoais no âmbito virtual, no entanto, limita-se a lei a subordinar apenas os entes da administração direta e indireta.

> Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
> I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;
> II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso. (BRASIL, 2011)

Ademais, com a expansão da internet tomando grandes proporções, a necessidade de uma discussão jurídica acerca das brechas em face do uso da rede para fins ilícitos tornou-se latente, assim, em abril de 2014 fora sancionada a Lei nº 12.965/14 (Marco Civil da Internet).

Assim, a lei dispôs sobre todas as condições de utilização e uso da internet, impondo responsabilidades na seara civil frente ao ambiente virtual, privilegiando os direitos à privacidade e dignidade, dando nova roupagem à proteção de dados no Brasil.

Com efeito, há de se ressaltar que o Marco Civil da Internet forma a grande base da Lei Geral de Proteção de Dados, ocasião a qual dá real início à nova era de proteção de dados, dispondo especificamente em seu art. 3º, qual seja:

> 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. (BRASIL, 2014)

A referida lei visa promover e regular o acesso à internet por todos os indivíduos, ressaltando a essencialidade do direito à privacidade e liberdade de expressão como garantia fundamental para o desenvolvimento da cidadania.

Ainda assim, demonstra a total preocupação do legislador em mais uma vez assegurar a inviolabilidade da intimidade e vida privada, recepcionando dispositivos que valoram a proteção de dados pessoais, uma vez que afirma que só deverá haver violação às comunicações realizadas no âmbito virtual em caso de ordem judicial, bem como dispõe acerca da transferência de dados à terceiros, citando que esta deve ocorrer apenas em caso de livre consentimento do titular do dado, observa-se:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> 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;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> 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;

> 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;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (BRASIL, 2014)

Portanto, após análise deste artigo 7º da citada lei, depreende-se a importância dada pelo legislador ao instituto da proteção de dados pessoais, acompanhando a grande evolução mundial acerca do tema, bem como aos diversos casos de lesividade ao consumidor virtual, que até então não maior importância jurídica acerca do tema, gerando grande influência na posterior Lei Geral de Proteção de dados.

No entanto, em que pese sua fundamental importância, há dispositivos na Lei do Marco Civil da Internet que necessitam de ainda mais especificidade em seu tratamento, a exemplo da proteção de dados pessoais dos indivíduos, surgindo então, a Lei Geral de Proteção de Dados (Lei nº 13.709/18), inspirada na legislação Europeia através do Regulamento Geral sobre a Proteção de Dados, dando novo e especial tratamento ao tema na tentativa de cessar as violações sofridas pelos usuários e impor uma nova era na segurança digital, ao passo em que observaremos as nuances desta lei em capítulo próprio, dada sua forte contribuição ao ordenamento jurídico brasileiro.

5 LEI GERAL DE PROTEÇÃO DE DADOS – UMA ANÁLISE SOB A PERSPECTIVA DA PROTEÇÃO DO CONSUMIDOR VIRTUAL

Conforme fora explicado em tópico anterior, em agosto de 2018 o presidente Michel Temer sancionou a Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados, a qual abarcou seriamente o tema e alterou dispositivos do Marco Civil da Internet, representando uma grande conquista para garantia de direitos fundamentais aos cidadãos que disponibilizam dados no meio virtual.

Tal importância e relevância do debate em razão da proteção de dados pessoais pode ser bem explicado quando olhamos para empresas como Google e Facebook, duas das mais rentáveis mundialmente, comum a ambas surge o fato de que a maioria do seu lucro advém de serviços gratuitos que coletam dados de seus usuários e são utilizados para a prática da publicidade direcionada.

O assunto se mostra de suma relevância tanto para os titulares dos dados quanto às empresas que fazem o tratamento, assegurando ao usuário o direito a sua privacidade, bem como a certeza da finalidade dada aos dados fornecidos, como exemplo citamos a possibilidade de o usuário exigir relatórios acerca do tratamento e armazenamento dos seus dados.

Assim como realizado pelo Marco Civil da Internet, a LGPD também trouxe conceitos técnicos acerca da temática, com o fim de equiparar a interpretação aos diferentes casos, sendo imprescindível o conhecimento acerca dos conceitos estabelecidos para uma boa análise da presente lei, conforme observa-se no artigo 5º:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (BRASIL, 2018)

Deste modo, percebemos a intenção da lei em proteger a pessoa natural na condição de titular dos dados pessoais, não sendo passível de extensão à pessoa jurídica.

No mesmo sentido, observa-se que a Lei nº 13.709/18 não tutela os dados anônimos, exemplificando que o conceito de dados pessoais pressupõe a titularidade de uma pessoa natural identificável, ressaltando que em caso de possibilidade de reversão do anonimato, este sim deve ser tratada como dado pessoal.

A lei torna-se de suma importância uma vez que consagra princípios fundamentais, aos quais serão mais bem explorados em tópico próprio, bem como dá

total controle ao titular do dado sobre a coleta e tratamento, através da necessidade de haver consentimento, igualmente o direito à retificação e apagamento.

A coleta de dados que anteriormente à LGPD era realizada de forma indiscriminada passará a ter regulamentação, uma vez que a lei determina a maneira a qual as empresas deverão tratar, repassar e até comercializar os dados obtidos.

O direito à privacidade passa a ser o mais tutelado com o advento da LGPD, o que até então era constitucionalmente garantido na era dos dados físicos passa a ter a devida importância também no meio virtual, acompanhando a evolução no mundo no tocante à proteção de dados pessoais, principalmente a legislação Europeia.

A proteção de dados pessoais é uma tendência mundial, assim, em razão da internet romper barreiras geográficas, se faz imperioso que os países aproximem suas legislações para que tal proteção seja efetiva, ocasionando em maior segurança ao consumidor/usuário no momento de suas trocas de informações.

Outro ponto importante a ser elencado é a previsão de pagamento de multa pecuniária, podendo a multa chegar até a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, algo extremamente positivo pois reforça a necessidade das empresas se adequarem, valendo ressaltar que as mesmas regras são aplicáveis para qualquer tamanho de empresas, bastando esta coletar e tratar os dados dos seus usuários.

Desta maneira, a LGPD fora consagrada com base em princípios que asseguram ao titular do dado o acesso aos seus direitos fundamentais, é neste sentido que iremos analisar a importância da lei para o ordenamento jurídico brasileiro sob esta perspectiva garantista.

5.1 Princípios norteadores

Os princípios que norteiam a referida lei têm sua referência no regramento europeu, sendo possível identificar vários pontos de convergência entre ambos. Assim, é fundamental uma análise pormenorizada acerca de cada princípio, a fim de entendermos a importância e capacidade da Lei geral de Proteção de Dados.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018)

Inicialmente, destaca-se os princípios da finalidade, adequação e necessidade, os quais citam que os dados devem ser tratados para um fim específico e informado ao titular, buscando garantir que os dados não sejam coletados e utilizados de forma ilimitada pelas empresas, sem qualquer controle do titular.

Acerca do princípio do livre acesso, conclui-se que deve ser garantida aos titulares o acesso facilitado e gratuito acerca da forma e o tratamento ofertado aos seus dados, assim, o controlador deverá atender a requisição no período máximo de 1 (um) mês, assegurando ao titular total autonomia acerca do tratamento dos seus dados.

Em relação ao princípio da qualidade dos dados, observa-se uma importante percepção do legislador ao afirmar que deve ser garantida a exatidão e clareza dos dados, incluindo-se aqueles também transformados, não somente os coletados, ou seja: todos os dados possuídos pelo controlador.

Já o princípio da transparência é fundamental e completa o direito ao livre acesso pelo usuário, desta forma, cita a lei que deverá haver clareza nas informações e tratamento de dados, cabendo ao titular o direito de solicitar seus dados pessoais e corrigi-los ou excluí-los de forma rápida e fácil, quebrando a burocracia costumeira.

Em relação ao princípio da segurança, este é considerado por muitos como o mais importante, haja vista o crescente número de casos de vazamento de dados ocorridos, desta maneira, as empresas detentoras dos dados devem disponibilizar meios capazes de assegurar ao usuário total segurança acerca dos dados ali inseridos, responsabilizando-os por eventuais vazamentos ou perdas acidentais.

O princípio da prevenção coaduna-se com o da segurança, uma vez que as empresas devem agir antes de ocorrer o dano, sob pena de negligência e consequente responsabilização civil, estes dois princípios reafirmam a necessidade dos fornecedores estarem em conformidade com a nova lei, tendo em vista a responsabilização civil decorrente das falhas e da mácula da imagem perante os consumidores.

O princípio da não discriminação encontra sua grande base no regramento europeu, vedando a utilização de dados sensíveis com fins que possam ser negativos ou discriminatório para o titular dos dados, demonstrando que a violação aos dados pessoais pode resultar em danos mesmo indiretos, assim, quando da descoberta da violação, deve a empresa comunicar imediatamente às autoridades.

Acerca do princípio da responsabilização e prestação de contas, este será o responsável por instituir a necessidade de as empresas estarem em conformidade com a lei, devendo haver uma regulamentação e adequação, bem como uma maior prestação de contas com as medidas tomadas para proteger os dados dos usuários, sob pena de responsabilização civil.

5.2 Responsabilidade civil no âmbito da proteção de dados

As relações humanas mudaram de acordo com a evolução da internet, cada vez menos temos a possibilidade de desassociar o real e o virtual, ambos estão entrelaçados no nosso cotidiano. Diante disso, há a inserção de uma grande massa de informações por parte dos usuários neste meio, sendo assim, a necessidade de tutela jurídica é latente, com a consequente responsabilização civil daqueles que insistem não dar o devido tratamento à esta garantia fundamental da proteção de dados.

Sendo assim, com o advento da Lei Geral de Proteção de Dados no Brasil, surge a necessidade de readequação do conceito de responsabilidade civil também para o âmbito virtual, especificamente da proteção de dados, estando o dever de

reparar os danos inseridos em circunstâncias novas, principalmente quando falamos em reparação pecuniária.

Deste modo, com o advento da LGPD e a possibilidade de reparar danos, as empresas devem ater-se cada vez mais à segurança dos seus usuários, reavaliando seus termos de uso e evitando vazamentos, sendo estas duas das prováveis causas de reparação pecuniária em decorrência de falha na proteção de dados, tendo em vista que a LGPD institui o dever de prestação de contas através de relatórios sobre o histórico de tratamento de dados fornecidos pelas empresas, bem como suas estratégias de segurança.

No mesmo sentido, um dos mais importantes institutos da LGPD encontra-se no art. 48, tendo em vista tratar-se da comunicação sobre o vazamento de dados, podendo gerar o dever de indenizar em caso contrário.

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. (BRASIL, 2018)

Ainda assim, será necessário verificar quais providências foram tomadas pela empresa, a fim de avaliar sua eficácia, pois este será um dos parâmetros avalizados no momento da responsabilização civil decorrente da falha de segurança.

Em prosseguimento, importante ressaltar a figura do controlador e do operador dispostos no art. 37 desta lei, sendo o primeiro responsável por decidir o que será feito com os dados e o segundo responsável por realizar o tratamento de dados, sob as ordens do controlador. Dito isto, entende-se que o fornecedor se divide em controlador e operador e o titular dos dados equivale ao consumidor nas relações consumeristas.

O artigo 42 da LGPD traz uma menção clara ao dever de indenizar, possuindo grande semelhança com o artigo 186 do Código Civil Brasileiro, analisando que o causador do dano deverá repará-lo, algo importantíssimo para a real eficácia da lei e garantir que o titular dos dados seja devidamente ressarcido do dano causado.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. (BRASIL, 2018)

O artigo 44 também é claro quanto a responsabilização civil, determinando as hipóteses em que haverá ato ilícito para que possa haver sua consequente apuração.

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. (BRASIL, 2018)

Sendo assim, observa-se que a responsabilidade do fornecedor é objetiva, não dependendo de comprovação de culpa para adquirir o dever de indenizar, tendo em vista que a empresa assume o risco ao coletar os dados, sendo seu dever obter mecanismos de segurança capazes de atenuar o máximo possível os riscos.

A LGPD não dispôs de critérios específicos para valorar uma possível indenização pecuniário, sendo assim, tal valor dar-se-á da junção de diversos aspectos, como a quantidade de indivíduos afetados, volume de dados afetados, métodos de segurança e prevenção empreendidos pela empresa, comunicação instantânea do fato à autoridade competente, entre outros diversos fatores que se coadunam com os princípios da lei.

Dito isto, infere-se que a necessidade de as empresas estarem em conformidade com a LGPD é uma necessidade concreta, tendo em vista que a evolução digital e as relações jurídicas dela derivadas são latentes. Assim, para que uma empresa se mantenha saudável e operando normalmente, deverá ater-se à Lei Geral de Proteção de Dados.

5.3 *Compliance* e LGPD

O advento da Lei Geral de Proteção de Dados promoveu grande impacto nas empresas atuantes no Brasil, sejam elas com plataformas virtuais ou não: todas coletam dados de alguma maneira. A referida lei colocou o País em um contexto de tendência global acerca da importância da proteção de dados.

Assim, em hipóteses de tratamento irregular de dados, as empresas terão diversas consequências, que vão desde a impossibilidade de contratar com o poder público às multas pecuniárias de alto valor, além de por óbvio trazer danos à imagem da empresa, caindo consideravelmente seu valor de mercado e faturamento.

Deste modo, considerando os estragos causados aos que não se adequar a lei, as empresas devem optar por programas de *compliance* a fim de evitar o

acontecimento de irregularidades e as consequentes sanções impostas pela lei, bem como a oportunidade de novos negócios.

Antes de prosseguir, devemos entender brevemente o conceito de *compliance,* o qual significa agir de acordo com uma regra, estar em conformidade com as leis do ordenamento externo e com as políticas internas da empresa.

Dito isto, entende-se que todas as empresas que se utilizam do tratamento de dados pessoais terão que investir fortemente em cibersegurança a fim de prevenir e detectar possíveis violações, principalmente quando analisados sob a vertente de que a adoção de práticas remediadoras será considerada no momento de uma sanção, podendo atenuá-la.

Assim, o fato de a LGPD entrar em vigor apenas em agosto de 2020, dois anos após sua publicação, fará com que as empresas tenham o tempo necessário a estar em conformidade, alterando suas políticas de segurança e seu código de conduta ética, capacitando seus profissionais sobre os novos regramentos.

Desta forma, um comitê de *compliance* deverá ser montado constituído por profissionais dos diversos setores da empresa, principalmente com forte apoio da área tecnológica, tendo em vista que esse profissional dará o aparato técnico necessário para elaboração das novas normas e capacitação dos funcionários.

Tal comitê irá implantar procedimentos para lidar com os dados pessoais dos seus clientes, com o objetivo de que sejam utilizados apenas os dados necessários para determinada função, seguindo o princípio da finalidade disposta na LGPD.

O consentimento deverá ser a pauta base no que tange às novas políticas da empresa, tendo em vista que deverá o comitê de *compliance* ao fato de que a lei permite que os titulares dos dados tenham total controle sobre estes, levando em conta que podem excluir, editar e que qualquer uso distinto tenha seu consentimento.

Um efetivo programa de governança deverá haver um monitoramento constante, possibilidade de revisão das informações a cargo do titular dos dados, bem como o cumprimento ao prazo de armazenamento.

Importante ressaltar que o programa de conformidade de uma empresa deve agir também em face dos seus fornecedores ou terceiros vinculados, tendo em vista que este poderá ser responsabilizado solidariamente em caso de irregularidades com seus fornecedores e terceiros vinculados.

Sendo assim, nota-se a necessidade das empresas de pequeno à grande porte estarem em conformidade com a LGPD, haja vista a importância do *compliance* para seus negócios comerciais.

Assim, entende-se que, mesmo diante das dificuldades impostas pela lei, estar em *compliance* com a LGPD é um grande investimento, haja vista a grande oportunidade de novos negócios, tendo em vista que tratar-se de um diferencial competitivo, aumentando sua reputação no mercado e principalmente perante seus consumidores.

6 CONSIDERAÇÕES FINAIS

O surgimento da internet constitui em um dos mais importantes marcos da humanidade, causando mudanças em todas as relações sociais, econômicas e culturais existentes. Assim, notório se falar que estamos cada vez mais inseridos nesse meio virtual, vivendo de fato em uma sociedade de informação.

Diante disso, o campo econômico tomou novas formas em face do surgimento do comércio eletrônico, com o consumidor beneficiando-se da redução de custos e possibilidade maior de escolha dos produtos, no entanto, imperioso destacar que esse novo campo também traz sérias fragilidades com relação à sua segurança, que vão desde fraudes à coleta indevida de dados pessoais.

Desta forma, os crescentes casos de vazamento de dados pessoais colocam em xeque a segurança do meio digital em decorrência de ações criminosas de *hackers* ou pela mercantilização desses dados, haja vista que o consumidor não possui real noção acerca do procedimento realizado em face da coleta e tratamento dos seus dados fornecidos.

Portanto, uma legislação eficaz para inibir as violações sofridas pelo consumidor no meio virtual era medida necessária, o ordenamento jurídico brasileiro não previa lei específica até o advento da Lei nº 13.709/18 – Lei Geral de Proteção de Dados – assim, o regramento dava-se apenas através de leis menos específicas como o Código de Defesa do Consumidor, Código Civil Brasileiro e o importante Marco Civil da Internet.

A preocupação legislativa acerca da proteção dos dados pessoais dos indivíduos é fundamental para assegurar que estes não sofram com irregularidades cometidas no meio virtual, através da coleta e fornecimento destes dados à terceiros sem o consentimento do titular.

Tendo em vista que com o crescimento da rede mundial de computadores, bem como a utilização de diversos outros tipos de meios eletrônicos, a coleta de dados atingiu patamares jamais vistos, sendo estes usados por diversas vezes para fins ilícitos.

Portanto, a LGPD vem para fechar as lacunas existentes no que tange à proteção de dados no ordenamento jurídico brasileiro, acompanhando a grande tendência legislativa mundial, inspirando-se no importante regramento europeu, o qual guarda muitas uniformidades com a lei brasileira.

Com isso, a LGPD protege a pessoa natural titular de dados pessoais, oferecendo total controle acerca da coleta e tratamento, tendo em vista o importante princípio do consentimento, o qual afirma que todo e qualquer tratamento ofertado aos dados do titular deve conter sua concordância, evitando assim que os dados sejam coletados e utilizados com finalidade diversa da esperada pelo titular.

Assim, privilegia a proteção ao direito fundamental da privacidade, o qual sofre várias violações em face da Revolução Digital ocorrida, ou seja, diante da democratização do acesso à Internet, bem como sua imprescindibilidade ao cotidiano do homem moderno.

Nesta senda, o consentimento do titular torna-se imprescindível e junta-se com o princípio da privacidade como os principais pilares da lei, tendo em vista deverá haver uma clara manifestação do titular para que haja a coleta e o tratamento dos dados.

A lei baseia-se em importantes princípios que asseguram ao consumidor uma maior segurança nos meios virtuais, consagrando o acesso aos seus direitos fundamentais, importante ressaltar que o conceito de consumidor confunde-se com o de usuário para os fins deste trabalho, haja vista a grande massa de coleta de dados tanto em compras instruídas por meios eletrônicos como em aplicativos gratuitos e de livre acesso.

Desta maneira, as empresas necessitam estar em conformidade com a presente lei, assim, investimentos em cibersegurança serão cada vez mais necessários diante da possibilidade de responsabilização civil.

Também há de se ressaltar as empresas responsáveis por aplicativos gratuitos nas plataformas digitais, haja vista a falta de transparência em face da coleta de dados dos seus usuários, principalmente em razão dos seus longos termos de políticas de privacidade expostos nas miúdas letras, aos quais o consumidor consente muitas vez apenas com o fito de utilizar a aplicação, sem qualquer conhecimento da finalidade dos dados coletados.

Em que pese a lei ainda não estar vigorando, sua eficácia é plenamente esperada tendo em vista o sucesso do Regulamento Geral de Proteção de Dados da União Europeia, a qual guarda significativas semelhanças com a LGPD.

Portanto, a lei é de suma importância para impedir que o consumidor sofra com as irregularidades cometidas no meio, dando-o total controle sobre a coleta e tratamento de seus dados e influenciando as empresas a investirem cada vez mais

na segurança dos seus clientes, representando grande avanço no ordenamento jurídico brasileiro, acompanhando a evolução da nova era digital.

Ademais, o fato de as empresas estarem em conformidade com a presente lei pode representar uma grande oportunidade de novos negócios, sendo considerado também um grande investimento, tendo em vista que a responsabilidade assumida pela empresa em relação à segurança trará grande confiança dos seus consumidores e fornecedores.

REFERÊNCIAS

BRASIL. Constituição da República Federativa do Brasil**. Constituição da República Federativa do Brasil.** Brasília, DF, outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 01 de setembro de 2019.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil.** Brasília, DF, janeiro de 2002. Disponível: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm> Acesso em: 01 de setembro de 2019.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Lei de Acesso à Informação no Brasil**. Brasília, DF, novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso: 01 de setembro de 2019.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Marco Civil Da Internet**. Brasília, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 23 de agosto de 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Brasília, DF, agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 01 de setembro de 2019.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Brasília, DF, setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm> Acesso em: 01 de setembro de 2019.

CASTELLS, Manuel. **A sociedade em rede.** 8. ed. São Paulo: Paz e Terra, 2005.

FORTES, Vinícius Borges. **Os direitos de privacidade e a proteção de dados pessoais na internet.** Rio de Janeiro: Lumen Juris, 2016.

GIANNASI, Maria Júlia. **O profissional da informação diante dos desafios da sociedade atual**. Brasília, 1999. Tese (Doutorado) - Universidade de Brasília, Brasília.

MARQUES, Claudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor: (um estudo dos negócios jurídicos de consumo no comércio eletrônico).** São Paulo: Revista dos Tribunais, 2004.

MENDES, Laura Schertel. **O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor**. Revista de Direito do Consumidor, São Paulo, vol. 106, jul./ago. 2016.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil – Análise** 2018. Disponível em: <https://baptistaluz.com.br/wp-content/uploads/2018/07/artigo-baptista-luz-pt-lei-geral-de Protec%CC%A7a%CC%83o-de-dados-do-Brasil.pdf>. Acesso em: 04 de agosto de 2019.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 6. ed. São Paulo: Atlas, 2013.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2010.

Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. – Rio de Janeiro: Forense, 2019.

PURKYT, Paulo. **Do que trata Lei de Proteção de Dados Pessoais?** 2018. Disponível em: <http://www.purkytveneziani.com.br/do-que-trata-lei-de-protecao-de-dados-pessoais/> Acesso em: 10 de agosto de 2019.

REDAÇÃO, ISTOE. **Uber pagará US$ 148 milhões por vazamento de dados**. [*S. l.*]: ISTOÉ DINHEIRO, 27 set. 2018. Disponível em: <https://www.istoedinheiro.com.br/uber-pagara-us-148-milhoes-por-vazamento-de-dados/> Acesso em: 21 ago. 2019.

ROMANI, BRUNO. **Procon multa Google e Apple por app que ‘envelhece‘ rostos**. [*S. l.*]: ESTADÃO, 30 ago. 2019. Disponível em: <https://link.estadao.com.br/noticias/geral,procon-multa-google-e-apple-por-app-que-envelhece-rostos,70002989532> Acesso em: 3 set. 2019.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais.** São Paulo: Edições Sesc, 2017.

YUGE, Claudio. **Facebook recebe multa de US$ 5 bilhões por vazamento de dados**. [*S. l.*: *s. n.*], 24 jul. 2019. Disponível em: <https://www.tecmundo.com.br/redes-sociais/144155-facebook-recebe-multa-us-5-bilhoes-vazamento-dados.htm> Acesso em: 20 ago. 2019.