UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA
COORDENAÇÃO DE MONOGRAFIA

TÚLIO ALECSANDER VICENTE SANTOS

PROTEÇÃO DE DADOS DO CONSUMIDOR COM ENFOQUE NO ÂMBITO DIGITAL

JOÃO PESSOA
2020

TÚLIO ALECSANDER VICENTE SANTOS

PROTEÇÃO DE DADOS DO CONSUMIDOR COM ENFOQUE NO ÂMBITO DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientador: Dr. Gustavo Rabay Guerra

JOÃO PESSOA
2020

Catalogação na publicação
Seção de Catalogação e Classificação

S237p Santos, Túlio Alecsander Vicente.
Proteção de dados do consumidor com enfoque no âmbito digital / Túlio Alecsander Vicente Santos. - João Pessoa, 2020.
52 f.

Orientação: Gustavo Rabay Guerra.
Monografia (Graduação) - UFPB/CCJ.

1. Proteção de dados pessoais. 2. Direito à privacidade. 3. Big Data. 4. Direito fundamental. 5. Publicidade direcionada. 6. Lei Geral de Proteção de Dados. I. Guerra, Gustavo Rabay. II. Título.

UFPB/CCJ

TÚLIO ALECSANDER VICENTE SANTOS

PROTEÇÃO DE DADOS DO CONSUMIDOR COM ENFOQUE NO ÂMBITO DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientador: Dr. Gustavo Rabay Guerra

DATA DA APROVAÇÃO: 27/03/2020

BANCA EXAMINADORA:

Prof. Dr. GUSTAVO RABAY GUERRA
(ORIENTADOR)

Prof. Ms. ADAUMIRTON DIAS LOURENÇO
(AVALIADOR)

Prof. Dr. ANDRÉ LUIZ CAVALCANTI CABRAL
(AVALIADOR)

Primeiramente a Deus por todas as bênçãos, e
segundamente à minha família por todo o amor
e apoio imensurável.

AGRADECIMENTOS

Inicialmente eu agradeço a Deus, por tudo de bom que tem me proporcionado, inclusive frutos da graduação. O Senhor sempre atendeu os meus pedidos, tudo conforme os seus planos.

Também agradeço aos meus pais, Maria do Socorro e Alessandro Zacarias, por todo amor e apoio. Sempre me amparando incondicionalmente. Obrigado de verdade por tudo, amo vocês!

Agradeço a minha irmã, Alessandra Vitória, pelo cuidado e amor, sempre à disposição para tornar minha vida mais tranquila e contribuir na realização dos meus sonhos. Amo você!

Aos meus avós, na pessoa de Aldecy Claro Monteiro, que mesmo de longe manteve seus cuidados e preocupações com seus netos. Amo todos!

Aos meus amigos, que de uma forma indireta contribuem para realização dos meus sonhos. Amo vocês!

E por fim, a minha namorada Ingrid Lohana, que apesar de ter chegado no finalzinho de uma fase, foi essencial para conclusão da mesma. Te amo muito.

“Não cometa o erro de achar que você é o cliente do Facebook, você não é – você é o produto. Os seus clientes são os seus anunciantes.”

Bruce Schneier

RESUMO

A proteção de dados é um tema que se tornou relevante em todo o mundo, tendo em vista que situações antes inexistentes passaram a fazer parte do dia-a-dia das pessoas, e isso mereceu atenção do Direito. Situações oriundas da evolução tecnológica mudou e muito a forma como as pessoas se relacionam, ocasionando o surgimento de novos perigos e problemas. Este trabalho tem como objetivo analisar até que ponto os dados das pessoas estão protegidos, dando ênfase ao consumidor, e no âmbito digital. Desse modo, foi realizado pesquisa bibliográfica e documental, por meio de livros, artigos, notícias e afins. Inicialmente foram trazidos conceitos necessários para a boa compreensão do trabalho, como *Big Data*, *Cookies*, e diferenciação de dados pessoais e dados pessoais sensíveis, posteriormente explanado acerca dos perigos e problemas inerentes à proteção de dados pessoais, e por fim a verificação da tutela das legislações pertinentes a temática, como a GDPR e a LGPD.

Palavras-chave: Proteção de Dados Pessoais. Direito à Privacidade. Big Data. Direito Fundamental. Publicidade Direcionada. Lei Geral de Proteção de Dados.

LISTA DE ABREVIATURAS E SIGLAS

CRFB/88 – CONSTITUIÇÃO FEDERAL
CDC – CÓDIGO DE DEFESA DO CONSUMIDOR
LGPD – LEI GERAL DE PROTEÇÃO DE DADOS
GDPR – GENERAL DATA PROTECTION REGULATION

SUMÁRIO

1 INTRODUÇÃO

Com o aumento exponencial da utilização dos meios eletrônicos, mudou-se a realidade da vida de todo o mundo, que passou de contatos reais, pessoais, para em grande parte, contatos digitais.

Devido a essa mudança, novas questões passaram a surgir, que merecidamente ganharam muita importância. Dentre elas, tem o que concerne à proteção de dados pessoais no âmbito digital.

Diante disso, se percebe a grande relevância de tratar acerca da proteção dos dados pessoais, tendo em vista que, com a evolução nas formas de relacionamento, sejam pessoais, sociais ou comerciais, os problemas tornaram-se outros.

Ora, se os meios das pessoas se relacionarem mudou, o direito que se adapta ao meio social e às novas realidades, também teve que mudar. Da mesma forma, essas evoluções também atingiram o consumidor, que inserido neste meio, se rendeu as facilidades.

Com isso em mente, é necessário verificar os novos problemas que surgiram, como também se de fato a legislação acompanhou as evoluções, dando enfoque principalmente na área consumerista, que já tem como característica inerente a hipossuficiência frente aos fornecedores.

Sendo assim, é imperioso ater-se a seguinte questão: o sistema jurídico brasileiro, de fato, salvaguarda os dados pessoais dos consumidores no âmbito digital? Há efetivas medidas de proteção?

O presente trabalho busca analisar as novas adversidades oriundas do contato entre os indivíduos e o meio digital, verificar se o direito já acompanhou essas mudanças na vida das pessoas, e trazer à tona se de fato há proteção no ordenamento pátrio. Partindo desde conceitos básicos, passando pelo surgimento dos novos perigos, até legislação que está na eminência de entrar em vigor.

Visando atingir tais objetivos, foi utilizado o método dedutivo, em que, analisando questões relevantes e possíveis, como também o ordenamento pertinente, associado à pesquisa documental indireta, a partir da coleta de informações mediante análise e revisão bibliográfica de livros, obras, artigos, sites, chegou-se a conclusões mais particulares.

Sendo assim, buscando tornar o trabalho de leitura agradável, no primeiro capítulo foi trazido diversos conceitos congruentes à temática, essenciais para uma boa compreensão de tudo que é apresentado. Partindo desde a definição de dados, até termos mais técnicos como *Big Data* e *Cookies.*

No segundo capítulo, foram demonstrados os novos perigos abarcados com a inserção de quase todo o mundo no meio digital. Desde o direcionamento de publicidade, até o vazamento de dados em massa.

Por fim, no terceiro capítulo, foi feita uma análise acerca das legislações aplicadas no que concerne à proteção de dados, demonstrando como se comporta o ordenamento jurídico brasileiro frente a essas novas questões.

2 ASPECTOS INTRODUTÓRIOS E CONCEITOS NECESSÁRIOS À PROTEÇÃO DE DADOS

Já não é mais novidade que vivemos em um mundo globalizado, chegando esse termo ser até um clichê de exacerbadamente ser dito, em que o Planeta Terra passou por um processo de integração, unificando-se em diversos aspectos, dentre eles os culturais, econômicos, sociais e digitais.

Muito dessa integração se deve à internet – conjuntos de dispositivos conectados em rede – por todo o mundo, tornando um planeta de milhares de quilômetros “pequeno” e sem fronteiras.

Acontece que, apesar dos diversos benefícios e facilidades trazidos por esse novo instrumento, que impactou com veemência a forma como vivemos, é necessário dar atenção a novas questões que antes não existiam.

Com essa interligação global proporcionada principalmente pela internet, o número de pessoas conectadas em um “único” ambiente atingiu um patamar jamais visto e que se supera a cada segundo. Percebe-se que é todo o mundo em um só meio que pode ser utilizado de formas inimagináveis. Desse modo, fica claro imaginar o número de informações que são transmitidas a cada milésimo de segundo.

Neste diapasão, tendo em vista o grande volume de informações e dados transmitidos diariamente, é imprescindível dar atenção a forma como tais são armazenados, manipulados e principalmente protegidos, ou pelo menos como devem ser. Ressaltando a importância do resguardo dos dados em si.

Importante lembrar o que está disposto no artigo 5º, inciso X da CRFB/88, veja-se:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (grifo nosso)

Nesse contexto, é claro e evidente a necessidade de proteção dos dados de todos os indivíduos que, dada a evolução tecnológica, mudaram a forma de inclusive armazenar a sua vida privada, saindo da coleção de fotos em álbuns físicos para armazenamento em espaços digitais, as conhecidas nuvens.

Diante de tal revolução, é importante focarmos no que concerne à proteção àquele já conhecido hipossuficiente: o consumidor. Este que, como não poderia ter

sido diferente, também aderiu às facilidades trazidas pela internet. Utilizando-a, por exemplo, tanto para compras online, como para interação com outras pessoas.

2.1 Termos técnicos

Inicialmente é importante trazer conceitos que serão necessários ao longo deste trabalho, para que se proceda com o seu bom entendimento, tendo em vista haver termos técnicos em diversos pontos, tanto os perigos que serão apresentados, como na legislação pertinente.

2.1.1 Dados x informação

A começar pelo de dados, que muitas vezes é trocado ou aplicado no lugar da palavra “informação” que é bem próximo daquele, mas que não deve ser confundido.

Podemos considerar “dado” como um termo puro, uma expressão mais primitiva que tem potencial de ser uma “informação”, podendo ser considerada um dado ou conjunto de dados que transmitem uma ideia sobre algo. Então, percebe-se que, para o dado se tornar uma informação, é necessário dar uma carga valorativa, seja qual for.

Desse modo, vários dados em conjunto para quem não tem interesse pode não significar nada, mas um simples para quem tem ideia de como utilizá-lo, seja para o bem ou para o mal, pode significar muito.

Nesta linha de pensamento, está o doutrinador Bruno Ricardo Bione (2020), veja-se:

> De início, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham sido utilizados de maneira intercambiável ao longo deste trabalho. O dado é o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação.
> Tome-se, novamente, o exemplo citado da multinacional Zara (vide subcapítulo 1.1.2). A simples ação de coletar e acumular os fatos (dados) das vendas e saídas de seus produtos é algo que em si não é dotado de nenhum significado. Somente quando organizados, especialmente para o fim de identificar quais produtos foram os mais

> vendidos, extrai-se, então, uma informação útil. Especificamente, quais produtos tiveram melhor aceitação pelo mercado consumidor para (re)projetá-los de acordo com tal tendência.

Verifica-se que para se extrair uma informação dos dados é preciso organizá-los, pois somente armazená-los sem nenhuma lógica, não possui significado algum. Eis que entra a questão do processamento que será conceituado em breve.

Agora trazendo uma definição técnica e pormenorizada de Valdermar W. Setzer (2005, p. 2):

> Definimos dado como uma representação simbólica (isto é, feita por meio de símbolos), quantificada ou quantificável. Assim, um texto é um dado, pois as nossas letras latinas formam um sistema numérico discreto (de base 26, que é o número de letras diferentes), e portanto quantificado. Mas uma foto também é um dado, pois é possível quantificá-la reduzindo-a a símbolos – pode-se digitalizar uma foto em um scanner e armazená-la em um computador, imprimindo-a posteriormente de modo que praticamente não se distinga do original. (...)
> Assim, uma foto de uma árvore é um dado (ou uma seqüência de dados). Mas é fundamental se entender que essa árvore em si, isto é, existente no mundo real, não é um dado.

Neste conceito, se percebe novamente que o dado é representação simbólica que recebe uma carga valorativa, assim, pessoas diferentes podem dar valores diferentes. O autor também chama a atenção para que o dado também pode ser uma representação de algo do mundo real, em que essa algo em si não é um dado, mas pode ser representado por um, seja uma foto, um vídeo, um desenho, etc.

No entanto, no presente trabalho, poder-se-á utilizar dos termos indistintamente nestes dois sentidos.

Também há definição de dados em um conhecido regulamento da União Europeia, no qual se referenciará mais futuramente, o Regulamento 2016/679, a conhecida GDPR – *General Data Protection Regulation*, que em Artigo 4º, 1), *in verbis*, dispõe:

> «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos

> específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

E um resumo dos conceitos, traz a LGPD – Lei Geral de Proteção de Dados, lei que em breve neste trabalho será explorada. Veja-se:

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

Agora analisando os conceitos trazidos nas legislações pertinentes à temática, se observa que o dado pessoal, é aquela já dita carga valorativa, no entanto, agora de uma pessoa, trazendo alguma informação acerca de um indivíduo. Existindo inclusive dados sobres questões intrínsecas da personalidade, que são os dados sensíveis que serão explanados no decorrer desde trabalho.

2.1.2 Banco de Dados

Feitas as considerações acima, se pode avançar para de onde são extraídos e armazenados os dados de que tanto se fala.

Os bancos de dados, em que podem ser definidos como o conjunto de dados armazenados, em uma estrutura organizada, com o desiderato de que, se relacionando entre si, criem algum sentido e tenham valor, ou seja, passam a ser uma possível informação extraível.

Mas para que essa informação seja extraída e se atinja o “conhecimento”, é necessário utilizar-se das ferramentas necessárias e passar por um processamento, que em amplo conceito é chamado de “mineração de dados”. Nome alusivo às minas de metais preciosos, conforme Leandro Nunes de Castro e Daniel Gomes Ferrari (2016, p. 4):

> O termo mineração de dados (MD) foi cunhado como alusão ao processo de mineração descrito anteriormente, uma vez que se explora uma base de dados (mina) usando algoritmos (ferramentas) adequados para obter conhecimento (minerais preciosos).

A alusão é perfeita para demonstrar o que são os dados e a necessidade de valorizá-los. De nada adianta ter somente a mina, se não tiver interesse em extrair os metais preciosos.

Desse modo, somente armazenar os dados em bancos, sem organizá-los, de nada servirá para extrair uma informação cognoscível.

A LGPD conceitua da seguinte forma:

> Art. 5º Para os fins desta Lei, considera-se:
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

O conceito da lei já traz os bancos de dados como estruturados, pois é justamente esse tipo de dado que merece atenção e proteção, os que podem trazer informações das pessoas, como também criar algum tipo de discriminação.

2.1.3 Tratamento de dados

Um outro conceito relevante para a boa compreensão do presente trabalho é o de tratamento de dados, que consiste em todos os procedimentos realizados com os mesmos.

Esse tipo de conceituação é fundamental para justamente compreender o processo que é realizado por diversas empresas, e analisar os riscos que podem ameaçar a privacidade do consumidor. É importante também pois contribui na distinção de possíveis práticas ilegítimas que violam o direito de personalidade dos indivíduos (MENDES, 2014, p. 94)

A própria Lei Geral de Proteção de Dados traz em seu corpo a definição de tratamento de dados. Veja-se:

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

O tratamento de dados é um processo dinâmico que abarca diversos procedimentos, buscando melhorar a informação para torná-la mais útil e consequentemente mais valiosa (MENDES, 2014, p.94).

Assim, qualquer manipulação de dados, independente do fim utilizado, pode ser considerado como tratamento de dados.

Para se valorizar os dados é necessário o tratamento deles, pois é o meio de definição de sua representação ante o fim que se almeja utilizá-los.

2.1.4 Processamento de dados

O processamento de dados é uma das fases do tratamento de dados. Como já explanado, de nada adianta coletar os dados se não forem postos a um refinamento, para torná-lo útil para determinada atividade. Esse refinamento é realizado por meio de técnicas de lapidação da informação, tornando um dado isolado, anteriormente sem utilidade, em uma potencial fonte de informação que pode contribuir para a captação de potenciais clientes pelas empresas.

Conforme explanado por (MENDES, 2014, p. 108), são diversas as técnicas que possibilitam a extração das informações:

> (...) como a *Datawarehousing*, *Data Mining*, *Online Analyticial Processing (OLAP)*, *Construção de Perfil (Profiling)* e *Sistema de avaliação (Scoring)*. Essas técnicas podem trazer benefícios e riscos ao consumidor. De um lado, a personalização de produtos e serviços e a possibilidade de obter publicidade direcionada aos seus interesses; de outro, riscos à privacidade, à discriminação do consumidor e à sua exclusão do mercado de consumo.

Aqui já se traz indícios dos possíveis riscos a que os consumidores possam estar expostos ao terem os seus dados processados e tratados, que merecem atenção tanto dos titulares desses dados como do sistema jurídico.

2.1.5 Dados pessoais x dados sensíveis

Importante trazer neste momento, a classificação dos dados em dois tipos, os pessoais e os sensíveis. Considera-se o dado pessoal como uma informação que

se remete a uma pessoa, ideia inerente a ela. Diferentemente dos dados anônimos, que por sua vez, são de pessoas não identificadas, que não dá para remeter a informação a um indivíduo.

Já os chamados dados sensíveis, estão contidos nos dados pessoais. Nestes tem que se dar uma atenção/proteção bem maior, pois o seu tratamento pode levar à discriminação de um indivíduo. Trazendo alguns exemplos, tem-se as opiniões políticas, dados relativos à vida sexual ou orientação sexual de uma pessoa, dados relacionados com a saúde física e mental, dados que transpareçam a origem racial ou étnicas, como também convicções religiosas ou filosóficas, dados genéticos e biométricos tratados para identificação do ser humano.

Neste sentido está a doutrina da especialista na seara da proteção de dados, a Doutora Laura Schertel Mendes (2014, p.43). Veja-se:

> Em outros casos, as normas retiraram da esfera do controle do indivíduo determinados assuntos, por compreenderem que alguns temas relativos aos dados pessoais são tão relevantes para o cidadão que merecem ser extremamente protegidos, não podendo estar na esfera de disposição individual. Tal pode ser observado na proibição, total ou parcial, imposta para o tratamento dos dados pessoais considerados sensíveis, que são aqueles cujo tratamento tem grande potencial de acarretar discriminação, tais como os dados relativos a etnia, opção sexual, opinião política e religião. (grifo nosso)

Percebe-se que a proteção no que se refere aos dados sensíveis, são tão essenciais que não se coloca à disposição dos detentores de tais dados a tutela dos mesmos, tornando-os indisponíveis, dado o grau de sua relevância.

Dentro dos dados sensíveis, importante destacar três: os genéticos, os biométricos e os relativos à saúde.

Quanto aos dados genéticos, traz a GDPR, em seu artigo 4º, 13), como os que concerne às características genéticas, hereditárias ou adquiridas, de um indivíduo singular, que dê informações únicas sobre sua fisiologia ou saúde.

Exemplificando, podemos citar CASTRO (2005, p. 94):

> Estes dados podem demonstrar, v.g., se duas pessoas são ou não da mesma família, podem revelar a presença ou ausência de uma característica num individuo, assim como a presença ou ausência do risco/probabilidade de doença.

Quanto aos dados biométricos, a GDPR, em seu artigo 4º, 14), conceitua da seguinte forma:

> (...) dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

Sendo assim, o dado que permitir a identificação por meio das características do ser humano, seja sua digital, retina, ou mesmo sua própria face, é um dado sensível.

E por fim, os dados relativos à saúde, que são aqueles que possam revelar informações sobre o estado de saúde de uma pessoa, seja física ou mental, incluindo os relacionados à prestação de serviço de saúde, como por exemplo uma ida ao hospital, vide artigo 4º, 15) da GDPR.

Diversos são os riscos que a exposição destes dados pode causar, levando inclusive a possíveis diversas formas de discriminação, como será em breve explanado neste trabalho.

2.1.6 *Big Data*

Feitas essas colocações, parte-se para mais um termo técnico essencial para o desenrolar deste trabalho. O chamado *Big Data.* Este conceito não é tão simples, tendo em vista que abarca outros para se chegar a sua definição.

Big Data é o termo utilizado para descrever uma grande carga de dados variados, estruturados ou não, que são gerados a cada milésimo de segundo por todos aqueles que estão no âmbito digital. Desde um só indivíduo, até empresas gigantescas.

Quando se fala em dados não estruturados, são aqueles que não têm qualquer relação entre si e nem uma estrutura definida, como é o caso de postagens em rede sociais, fotos, vídeos, textos, e até a geolocalização.

Essa ferramenta é utilizada desde a tomada de decisões no que concerne ao futuro de grandes corporações, como também para o direcionamento de publicidades para o consumidor internauta.

Os termos que constituem o *Big Data* no geral são três: Volume, que consiste na grande quantidade de dados que são gerados por milésimo de segundo; Velocidade, que se trata da obtenção e análise dessa grande quantidade de dados em tempo real; e Variedade, que consiste nas diversas fontes que tais dados são obtidos.

Importantes considerações fez Bruno Ricardo Bioni (2020), em sua doutrina, sobre o *Big Data*:

> Com base no que já foi mencionado sobre o progresso quantitativo e qualitativo da gestão da informação (vide subcapítulo 1.1.1), seria possível dizer que o Big Data representa o êxtase desse processo. Essa tecnologia permite que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades. Com base na abordagem de Doug Laney, o Big Data é comumente associado a 3 (três) "Vs": volume, velocidade e variedade. Volume e variedade, porque ele excede a capacidade das tecnologias "tradicionais" de processamento, conseguindo organizar quantidades antes inimagináveis – dos bits aos yottabytes – e em diversos formatos – e.g., textos, fotos etc. – e, tudo isso, em alta velocidade.
> (...) Em conclusão, Big Data não se preocupa com a causalidade de um evento, mas, tão somente, com a probabilidade de sua ocorrência. Em vez de questionar por que algo acontece, procura-se diagnosticar o que está acontecendo. Não se está preocupado com a análise das razões que geram uma cadeia de eventos, mas, tão somente, com o seu desencadeamento.

Ante excelente explanação fica claro que esta ferramenta tem como objetivo "prevê" se um fato vai acontecer ou já está acontecendo, para direcionar as atividades no interesse da empresa. Seja a venda de um produto, seja evitar uma crise financeira.

Aqui, o risco ao consumidor está justamente no rastreamento dos seus dados, que podem ser utilizados para direcionamento de publicidade, pode até cercear o poder de escolha do consumidor, que será bem explanado no próximo capítulo desde trabalho.

2.1.7 *Cookies*

Um conceito que não pode faltar é dos Cookies, um tipo de arquivo rastreador que tem seus benefícios e malefícios.

Funciona da seguinte forma: ao acessar uma página na internet, pequenos arquivos são armazenados vinculadas a ela, a fim de identificar qual internauta está acessando no momento. Um exemplo é ao acessar um site e automaticamente o *login* e senha serem preenchidos, é o *cookie* armazenado ao entrar pela primeira vez neste site que permitiu isso.

O objetivo é personalizar a página de acordo com o perfil do usuário, ou mesmo facilitar o transporte de dados entres as páginas desse mesmo site (ALVES, 2018).

O problema é que não há qualquer limite sobre às informações que estão sendo registradas, que vão de um endereço de e-mail até a localização do indivíduo que está a permitir a ação do *cookie*.

Cita-se a definição dada por MENDES (2014, p. 102-103):

> Os cookies são marcadores digitais que são automaticamente inseridos por websites visitados, nos discos rígidos do computador do consumidor, em sua casa ou no seu local de trabalho, para possibilitar a sua identificação e a memorização de todos os seus movimentos. Agem quase sempre sem que o internauta tenha conhecimento, podendo trazer benefícios ou malefícios, conforme o caso. Por um lado, são os cookies que permitem aos internautas a memorização de senhas e a personalização de serviços. Por outro, quando o computador é associado aos dados do internauta, a partir de seus dados pessoais fornecidos a um determinado site, esses marcadores tornam-se ameaçadores à privacidade. Ademais, quando inseridos por um longo período, os cookies possibilitam o rastreamento do comportamento do usuário em diversos sites.

Os *cookies* possuem duas vertentes, tanto a de facilitar e personalizar o acesso do usuário, como também de rastreá-lo justamente para estes fins. Ou seja, nada mais é do que colocar os dados à mercê de outros visando facilidades no dia-a-dia. Mas por meio dele, se percebe o quanto as pessoas são monitoradas, inclusive sem perceber, e isto é um risco.

Os *cookies* não devem necessariamente deixar de serem utilizados, pois também traz benefícios, mas é necessário que deixe o titular do dado ciente das utilizações, e que haja limites legais para isso, pautando sempre pela transparência e autorização.

3 DADOS PESSOAIS: CAPTAÇÃO, UTILIZAÇÃO E PERIGOS

Feitas as explanações necessárias, agora será apresentado de fato a origem da problemática do presente trabalho que é a captação e possíveis formas de utilização dos dados pessoais dos consumidores indistintamente.

Pode-se considerar que a atual era é a da informação, e este título não é à toa. Os dados pessoais dos cidadãos tornaram-se um fator vital para a economia no mundo, principalmente no que diz respeito ao enaltecimento dos bens de consumo, que é o marketing, como também a divulgação destes, no caso a publicidade. (BIONI, 2020).

E para deixar mais claro ainda o porquê que as informações foram se tornando tão relevantes, se traz uma metáfora extraída da obra de Bruno Ricardo Bioni (2020), que também dá um *insight* acerca da utilização dos dados. Veja-se:

> Scoopville era uma cidade famosa pela produção de sorvetes. Todos os seus moradores produziam os seus próprios “gelatos”, cujos sabores variavam de acordo com as suas respectivas preferências. (...)
> No entanto, os visitantes ficavam simplesmente desnorteados com o volume de opções. Até que um dos comerciantes teve a ideia de colocar um painel, em frente à sua loja, para que os consumidores emitissem as suas opiniões sobre os diversos tipos de sorvetes.
> Esses comentários passaram a influenciar não só o consumo por parte dos novos visitantes da cidade, mas, principalmente, a própria fabricação do produto. (...)
> A Internet e a sua camada de aplicações, principalmente a web com blogs, redes sociais, websites etc., capilarizou esses painéis de opiniões. Os consumidores compartilham e trocam, com mais frequência, em diversos canais e quase em tempo real, informações sobre as suas experiências de consumo: (...) Em todas essas situações, eles passam a ser “ouvidos” por seus milhares de pares, parametrizando o próprio movimento de consumo.
> O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa, que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do *prosumer*. O consumidor não apenas consome (*consumption*), mas, também, produz o bem de consumo (*production*): *prosumer*.

E isso fica bem claro com a existência de sites como o reclameaqui.com.br, site brasileiro que oferece o serviço gratuito para os consumidores postarem suas reclamações e darem o *feedback* acerca de uma marca, produto, ou serviço prestado por uma empresa, existindo inclusive um *ranking* das mais reclamadas.

Ademais, quem nunca buscou no Google: “Empresa tal é confiável?” “Produto tal, é bom?”. Isso é reflexo justamente da participação ativa do consumidor, sendo, portanto, este, até que um ponto positivo da inclusão massiva. No entanto, há diversos riscos perante os grandes números de informações que são colocadas à disposição na internet, que é o que será visto agora.

3.1 Meios de captação de dados e formas de utilização

Que os dados são extraordinariamente valiosos, isso está claro, mas como estes são captados e por que são tão preciosos assim?

Como dito, o mundo está em constante evolução, isso inclui dentre outras áreas, as econômicas. Com o advento da internet, viu-se um meio bastante propício a lucrar, e logo inúmeras formas de se aproveitar disso foram criadas, dentre elas a utilização de dados para diversos fins.

Com uma participação maior dos consumidores no âmbito digital, consequentemente aumentou o fluxo de dados nas redes. Com isso os riscos a que as pessoas estão expondo os seus dados, são maiores, podendo ser utilizados de inúmeras formas.

O consumidor precisar estar atento isso, como também tem que ter a sua disposição mecanismos de defesas, como legislações e órgãos competentes.

Ante isso, agora será visto alguns dos meios de captação e utilização de dados, visando lucro ou benefícios dos detentores dessas infinitas informações, como também será demonstrado os riscos inerentes a esse tipo de atividade.

3.1.1 A utilização de *Cookies*

Tendo em vista se estar na era da informação, com o meio digital invadindo a vida das pessoas mais do que nunca, a publicidade também passou a utilizar-se desse meio.

Publicidade é uma estratégia de marketing que consiste na compra ou aluguel de um espaço a fim de divulgar um produto, serviço ou marca, tendo por objetivo atingir um público-alvo e fazê-lo com que compre. (CASAROTTO, 2019).

Não há meio mais interessante do que a internet para se fazer publicidade, tendo em vista a forma de como ela é utilizada e por ter bilhões de usuários em todo o mundo.

A publicidade direcionada, que é aquela personalizada correlacionada com um determinado fator que dá mais chances de atingir êxito, pode ser dividida em três tipos: contextual, segmentada e comportamental.

A contextual correlaciona o ambiente destinado à publicidade com o objeto anunciado, seja numa revista, seja em um jornal. Desse modo, direciona tal processo comunicativo de um produto em um ambiente de pessoas que tem mais tendência em adquiri-lo, como exemplo, publicar a venda de um carro em uma revista sobre carros. A publicidade segmentada foca no subjetivo, ou seja, diretamente no público que se almeja atingir, não sendo importante o ambiente e sim quem frequenta ele. Desse modo, se segmenta a publicidade a uma determinada massa de consumidores. E por fim, a mais importante para este trabalho, a chamada publicidade comportamental online, em que, por meio dos instrumentos tecnológicos, dentre eles os *cookies*, tornou-se possível identificar em que o internauta navega a fim de verificar seus interesses e correlacioná-los aos anúncios publicitários (BIONI, 2020).

Importante trazer a citação da *Federal Trade Comission* norte-americana realizada por Danilo Doneda no Caderno de Investigações Científicas com a temática “A proteção de dados pessoais nas relações de consumo: para além da informação creditícia”, da Escola Nacional de Defesa do Consumidor , em que afirma ser o conjunto de hábitos do usuário na internet uma das fontes de dados mais visadas:

> A publicidade comportamental é o monitoramento das atividades de um consumidor quando conectado à Internet - incluindo as pesquisas que ele fez, as páginas que ele visitou e o conteúdo consultado - com a finalidade de fornecer-lhe publicidade dirigida aos interesses individuais deste consumidor.

Ao acessar a internet, todos os “passos” dados pelo consumidor estão sendo monitorados, a fim de descobrir quais são seus interesses de compra. Desse modo, ao direcionar a publicidade de um produto que foi pesquisado pelo internauta, a probabilidade de a compra ser realizada é maior. Com isso, o fornecedor acaba economizando nos gastos de difusão do seu produto, como também aumenta o seu número de vendas. Isso é totalmente benéfico para o fornecedor, mas é arriscado para o consumidor.

Trazendo novamente a temática dos *cookies* que se encaixa perfeitamente ao tipo de publicidade comportamental online, também conhecida como *Online Behavioral Advertising – OBA,* é importante discorrer a forma como esta ferramenta funciona.

Ao navegar por um site qualquer que possui *cookies,* toda navegação do usuário passa a ser rastreado, pois este começa a enviar ao navegador diversas informações acerca da utilização por parte do indivíduo. E não há qualquer limitação, pois se pode registrar, desde senhas e logins, como também a localização, por exemplo.

Apesar de ter alguns benefícios, o que se percebe é que há mais malefícios, sendo imperioso ressaltar que se trata de dados pessoais, sendo inclusive alguns deles sensíveis, o que merece atenção ao ser disponibilizado de qualquer maneira.

Os *cookies* fazem com que, ao entrar numa página, seu login e senha já estejam preenchidos, as notícias de um site já remetam a sua localização, os anúncios publicitários sejam relacionados a região em que está no momento, dentre outros. O que se verifica é que há uma troca de dados por comodidade. E o que é mais importante, acessar um site e ele já estar todo personalizado à sua maneira, ou não ter a dúvida de que os seus dados estão em segurança? Tal questionamento deve variar de pessoa para pessoa.

Um outro exemplo de uso de dados pela utilização de *cookies* no sentido da publicidade comportamental, é quando se pesquisa algum produto de interesse, seja um computador, um tênis, um produto de beleza, e ao sair da página, ao visitar outras, o usuário é bombardeado de publicidades do produto que acabou de realizar a pesquisa. Ou seja, por meio do *cookie* do site de venda, uma empresa que processou os dados, “informa” ao canal publicitário que concede o espaço à vendedora, o produto de interesse do consumidor internauta, que tem mais chances de comprar, tendo em vista que o mesmo acabou de pesquisar.

Desse modo, fica claro o mapeamento da navegação que o *cookie* realiza, formando o perfil do consumidor, para que se possa apresentar a este, anúncios personalizados, aumentando assim, o percentual de probabilidade de compra, ao invés de despender tempo e dinheiro com uma massa de consumidores que sequer tem interesse em adquirir tal produto.

São condições primárias para constituição da publicidade comportamental, a coleta, junção e armazenamento das informações sobre os consumidores, pois com

tais dados se cria um perfil e se destinam mensagens publicitárias sob medida, dentro de interesses que provavelmente são maiores. Tudo isso sendo caracterizado a partir de seus hábitos e atos. (DONEDA, 2010, p. 63).

Conforme delineado por Danilo Doneda, para se criar o perfil do consumidor, é necessário a captação dos seus dados, para traçar os seus maiores interesses. No entanto, um dos riscos maiores é justamente não estar sendo demonstrado todos os produtos de interesse do consumidor, e sim os interesses dos fornecedores, proporcionando somente a estes o poder de escolha do que ofertar.

3.1.2 As redes sociais

Como se sabe, para ingressar na maioria das redes sociais é requisito mínimo fornecer nome, e-mail e criar uma senha. Bom seria se tudo parasse por aí, mas provavelmente não se tornaria uma rede social.

O número de dados e informações que os usuários passam para as redes sociais, são inimagináveis. Desde rotina diária, páginas de interesse, estilo de música, lugares frequentados, publicação de fotos, vídeos, opiniões etc. Não sendo estranho dizer que vez ou outra, crimes diversos contra pessoas são cometidos após análise de sua vida digital, já que a maioria demonstra seu dia-a-dia nas redes.

Se os dados captados fossem somente o que são publicados pelos próprios usuários, já seria grave, mas ainda assim se teria certo controle sob o que é exposto a todo o mundo, no entanto, o problema é bem pior, pois todos os dados que passam pelas redes sociais, são utilizados, até os que não se possa imaginar, como a localização do usuário, páginas acessadas dentro da rede, e até comunicações com outros usuários, etc.

Um exemplo gravíssimo é o fato de o Facebook ter assumido escutar e transcrever conversas de áudio do Messenger, por meio de funcionários terceirizados, a fim de avaliar se a inteligência artificial da rede social estava funcionando corretamente, conforme notícia da Época Negócios Online (2019):

> Depois das gigantes Microsoft, Amazon, Google e Apple, o Facebook entrou na lista das big techs que estão ouvindo — e transcrevendo — conversas que os usuários têm com seus sistemas de assistentes virtuais. Nesta semana, a rede social admitiu contratar funcionários terceirizados para o serviço.

> Segundo a empresa, o trabalho tinha como objetivo avaliar se a inteligência artificial interpreta corretamente as mensagens recebidas e responde de forma satisfatória aos pedidos dos usuários. De acordo com o Facebook, o sistema foi suspenso depois da repercussão negativa das notícias de que outras empresas tinham políticas similares com suas assistentes de voz. "Assim como a Apple e o Google, paramos a análise humana do áudio há mais de uma semana", afirma em comunicado.
> A opção de áudio pelo Messenger foi implantada em 2015 na plataforma. De acordo com o Facebook, os usuários são notificados de que as informações trocadas pelo aplicativo serão "automaticamente processadas" para análise do contexto e conteúdo. No entanto, não fica claro que o processo é feito por humanos. Os funcionários encarregados da transcrição não tinham acesso aos dados dos usuários.

Apesar de ser alegado que o uso é somente para aprimoramento da inteligência artificial, o que garante que estes dados não estão sendo utilizados para direcionamento de publicidades? Afinal, quem nunca se deparou com uma publicidade no Facebook ou qualquer outra rede social, quando acabara de conversar sobre algo? E o problema pode ser pior, se estiverem utilizando dessas mensagens para identificar possíveis pontos de discriminação de usuários dessa rede.

Outro fato é que o Facebook tomou a mesma medida de outras empresas do segmento online ao ser descoberta: suspendeu o serviço temporariamente. E isso demonstra pelo menos indícios de atitude suspeita. Por que suspender um serviço que está totalmente dentro da legalidade e não fere a privacidade e consequentemente a personalidade dos seus usuários? Não há coerência.

Por oportuno, também se lembra que a referida empresa já foi multada no valor de 5 bilhões de dólares por falhas de privacidade no caso Cambridge Analytica, em que de acordo com a investigação, os usuários da rede social ao responder um quiz, deram permissão para que este tivesse acesso aos dados pessoais que posteriormente foram fornecidos a uma empresa que utilizou na campanha eleitoral de Donald Trump.

Não é somente o Facebook que já que admitiu analisar dados dos usuários, gigantes como a Google, Apple e Microsoft, também admitiram se utilizar desses métodos. Para quem não sabe, o sistema Android é da Google, então toda vez que se utilizava da assistente pessoal "Ei Google", os áudios estavam sendo utilizados. Do mesmo modo para "Hey Siri" e "Olá Cortana", da Apple e Microsoft respectivamente.

Agora partindo para um outro de tipo de aplicativo que pode ser considerado como uma rede social diferente, é o Waze, aplicativo de navegação que é alimentado pelos usuários sobre as rotas e tudo que contém nelas, desde radares até acidentes, como também o fluxo do trânsito. Esse *app* se utiliza da localização do usuário para guiá-lo seja na cidade ou na estrada. Quando permitido, também monitora a localização mesmo sem estar utilizando-o, com o intuito de avisar o usuário a hora que deve sair, já analisando o trânsito, para que não haja atrasos.

Apesar do seu uso ser bem interessante, o aplicativo também se utiliza da publicidade direcionada, pois remete ao usuário propaganda de estabelecimentos que pagaram pelo espaço publicitário. Então, ao estar próximo de algum lugar de interesse do Waze, se demonstrará uma publicidade na tela do *smartphone,* sem o usuário pedir, para que este tenha interesse em ir ao destino demonstrado, ou seja, influenciando no poder de escolha, e até mesmo de vontade.

Ante essas explanações, fica claro os riscos a que os usuários estão submetidos ao utilizarem as diversas redes sociais existentes, em que, além das informações que são oferecidas, as empresas se utilizam dos mais diversos dados em benefício próprio, seja para aprimoramento de seus recursos, seja para venda a outras empresas interessadas em publicidade. Isso demonstra uma clara transgressão aos direitos tabulados na Constituição Federal e outros dispositivos do ordenamento pátrio, pois nesses casos não estão se importando com a privacidade do seu usuário, e sim em lucrar por meio dos dados que são fornecidos, tendo em vista que estão recebendo e muito por isso.

3.1.3 Cadastro por meio do CPF

Outro meio de captação de dados é por meio da utilização do CPF - Cadastro de Pessoa Física, que é um documento emitido pela Receita Federal que serve para identificar os contribuintes. Consistente em uma numeração com 11 (onze) dígitos, que permanece durante toda a vida do indivíduo, mudando somente por meio de decisão judicial.

Além de identificar os contribuintes na declaração do Imposto de Renda, o CPF é um dos documentos essenciais para qualquer pessoa. Sendo utilizado nas mais diversas formas, inclusive identificação do portador, como exemplo para abertura

de conta, matrícula na universidade, cadastros nos mais diversos órgãos governamentais, etc.

Acontece que, além da utilização do CPF para esses fins, que querendo ou não são essenciais, percebe-se que as pessoas o utilizam na maioria das vezes desnecessariamente e sem perceber, que são naqueles casos em que estabelecimentos comerciais solicitam o documento para efetivação da venda ou de um desconto, ou por simplesmente pedir.

Por exemplo, ao realizar a compra em uma farmácia, para ativar o desconto é necessário realizar cadastro e fornecer o CPF. Da mesma forma acontece ao se fazer compras no supermercado, mais utilizado principalmente para somente “colocar o CPF na nota fiscal”.

Por ser algo bem simples, o fornecimento de uma numeração para identificação, nem parece que por trás há perigos no que concerne à utilização de dados pessoais sensíveis, perigos estes que serão demonstrados no subcapítulo a seguir.

3.2 Perigos relacionados à captação de dados

Conforme já delineado, uma das formas mais lucrativas que a utilização de dados pessoais permite, é por meio da publicidade direcionada, em que, com a coleta dos mais diversos dados dos consumidores se criam perfis que caracterizam o consumidor a partir de seus hábitos e atos.

O problema da utilização de dados dessa forma é que influencia a interação do usuário, pois faz com que seja somente veiculada a publicidade que mais se adeque ao perfil do consumidor, o que pode limitar o rol de escolhas futuras destes a partir de um perfil que foi “calculado” por um comportamento anterior (DONEDA, 2010, p. 68).

Podemos até considerar isso como um cerceamento do poder de escolha, em que dentre as diversas opções em que o consumidor possa ter interesse, só é demonstrado aquela que pagou para aparecer.

Conforme apontado por Danilo Doneda (2010, p. 68):

> Este fenômeno já chegou a ser denominado de *boxing*, segundo a metáfora de que as possibilidades oferecidas a uma pessoa são

> fechadas - encaixotadas - em torno de presunções realizadas por ferramentas de análise comportamental, guiando desta forma as suas escolhas futuras. A publicidade assim encaminhada teria o efeito colateral de uniformizar padrões de comportamento em torno de padrões definidos pelos algorítimos (sic) e categorias utilizadas por tais ferramentas, diminuindo de fato a diversidade e o rol de escolhas apresentados a uma pessoa.

Lembrando que a tendência é ser publicitado o produto daquele fornecedor que comprou o espaço, e está se utilizando dos dados fornecidos para vender o seu produto, então não significa que vai ser direcionado ao consumidor o de menor preço, muito menos o de melhor qualidade, diminuindo assim, consideravelmente as possibilidades de compra.

Também se pode imaginar que essa segmentação da publicidade atinja inclusive no que se refere aos noticiários jornalísticos, em que com o oferecimento de notícias personalizadas, direcionando somente possíveis tópicos que o leitor possa se interessar, elimina-se o acesso a outros tipos de informação em que eventualmente lhe interessaria, mas que não é demonstrado (DONEDA, 2010, p. 68). Ou seja, aqui aparece um novo tipo de limitação, que é o da informação, e isso é bastante grave, pois influi e muito nos moldes de personalidade de um indivíduo.

Uma outra atividade que pode ser questionada, existente a partir da personalização das pessoas por meio de seus dados, é a variação do preço a ser cobrado de pessoa para pessoa – chamado (*adaptative pricing*) – por um produto ou serviço, em que se identifica quem estaria disposto a pagar mais por possuir um perfil inclinado a isso (DONEDA, 2010, p. 69). Sendo tal atitude uma afronta direta a CF – Constituição Federal em seu Artigo 5º Caput, que diz que “todos são iguais perante a lei”, como também ao Código de Defesa do Consumidor (Lei 8.078/90), em seu Artigo 6º, II, que declara ser direito básico do consumidor “a igualdade as contratações”. Não há possibilidade de igualdade nas contratações se os preços estão discriminatoriamente diferentes.

Diante disso, por meio da dedução, se pode levantar novas questões acerca da utilização de dados das mais diversas formas. Em relação à utilização do CPF, nos cadastros ou em simples compras, o perigo mora no sentido de, se tais dados estiverem sendo utilizados também para criar um histórico dos consumidores, para inclusive realizar uma diferenciação no preço. Por exemplo, o consumidor realiza compra constante de um determinado remédio que em uso durante vários anos pode

ocasionar outros problemas de saúde, e esse tipo de dado/informação seja repassado para os planos de saúde que ele possa vir a contratar, e assim, estes cobrem um valor superior por justamente o consumidor se utilizar desse remédio. Um outro exemplo é em relação a compras no supermercado, em que ao vincular o CPF na nota fiscal, todos os produtos durante toda a vida do consumidor fiquem registrados, fazendo com que novamente empresas voltadas para a saúde façam um mapeamento do possível estado de saúde deste consumidor com base em suas compras, a fim de diferenciar o valor a ser cobrado em um possível atendimento.

Apesar de serem possibilidades, a tendências de coisas como essa e até outras inimagináveis acontecer ou já estarem acontecendo, é grande. Ora, esse tipo de atividade interfere diretamente no lucro de empresas, que estão sempre em busca de métodos para ganhar cada vez mais.

Analisando bem, já existe esse tipo de atividade na área econômica, como é o caso dos órgãos de proteção de crédito – SPC e Serasa – que tem a função de registrar em seus bancos de dados, as pessoas que contém dívidas atrasadas ou não. O objetivo é dar informações as instituições financeiras ou empresas comerciais, acerca do status financeiro do indivíduo, para que se proceda ou não com a concessão de crédito. Inclusive, as pessoas recebem uma pontuação denominada *Score,* que consiste em sua nota dentro do mercado financeiro e comercial, em que, quanto maior o *Score* maior a credibilidade. Para constituição dessa pontuação é levado em conta o nível de adimplemento, valores contratados, movimentação financeira, etc.

Um outro risco inerente ao armazenamento de dados são os vazamentos, que consiste na exposição dos dados de diversas pessoas sem o seu consentimento, seja por ataques de *hackers* criminosos*,* seja por falha de segurança dos detentores das informações expostas. Se já é perigoso o fornecimento de diversas informações a empresas que temos o conhecimento, imagina com uso indevido por qualquer pessoa que roubou os dados pessoais de milhares.

Já se sabe como a proteção aos dados é imprescindível, tendo em vista as diversas formas maléficas que eles podem ser usados. Então quando se fala em vazamento, pode ser qualquer tipo dado, desde biométricos, como telefônicos, sensíveis, qualquer um. E isso é de uma preocupação enorme, um ponto em que as leis devem dar um foco maior.

Não é raro encontrar casos de vazamento de dados envolvendo milhões de vítimas, como é um dos casos do Facebook, revelado em setembro de 2018, em

que informações de perfil, crenças políticas, rede de amigos e mensagens privadas de 87 milhões de usuários dessa rede social foram expostos. Sendo este o famoso escândalo da Cambridge Analytica, em que a empresa de coleta de dados captou sem autorização informações dos usuários, por influência da campanha presidencial americana de 2016 (Hron, 2019).

Ainda sobre esse caso, foi realizado um teste de personalidade com milhares de pessoas, e os dados captados vendidos à Cambridge Analytica, sendo utilizados possivelmente para catalogar o perfil das pessoas e direcionar de forma mais personalizada, materiais a favor de um candidato e outros contra o adversário (BBC, 2018).

Ante isso, novamente se reitera o perigo do armazenamento de dados e a sua possível falta de proteção. Mais uma vez, percebe-se que os dados podem constituir informações importantíssimas, e indubitavelmente merecem extrema proteção.

Feitas essas explanações dá para perceber o quanto a manipulação indevida dos dados é perigoso para os titulares destes. Chegando inclusive a ter a possibilidade de discriminação.

Isso é um problema emergente justamente das novas formas de comunicação e também transações comerciais permitidas pelo advento da internet, ou mesmo práticas comuns do dia a dia, como é o caso da utilização do CPF.

Tendo o conhecimento acerca desses novos riscos, é preciso a sociedade em geral atentar para que se a legislação vigente, de fato, está tutelando os dados pessoais, com as devidas medidas de proteção.

Ora, os dados pessoais refletem diretamente a personalidade do indivíduo, que pode até ser, em casos extremos, discriminado, como ter também invadida a sua privacidade, então, é dever do estado proteger esse direito fundamental.

Com isso mente, no capítulo que se inicia logo a seguir, será demostrado as legislações específicas do Brasil, que tratam acerca da proteção de dados. Ademais, também será analisado se essas legislações são suficientes e se de fato funcionam, ou o que precisam para funcionar, trazendo as hipóteses do problema que está a se discutir.

4 LEGISLAÇÕES APLICADA À PROTEÇÃO DE DADOS PESSOAIS

Conforme todas as explanações aqui realizadas, não há dúvidas de que os dados pessoais são preciosos e precisam de proteção.

Neste capítulo será abordado justamente se os dados pessoais estão legalmente salvaguardados, e até que ponto estão.

4.1 Direito à privacidade: proteção à inviolabilidade da personalidade

Para iniciar qualquer discussão acerca da tutela dos dados pessoais, é essencial trazer inicialmente o debate sobre o direito à privacidade e sua proteção, com a inviolabilidade da personalidade.

Como aconteceu nos tempos atuais, em relação à proteção de dados pessoais, foi em decorrência do surgimento de novas técnicas e instrumentos tecnológicos que iniciou as discussões doutrinárias acerca da privacidade, pois tais ferramentas passaram a permitir a divulgação de fatos relativos à esfera privada do indivíduo de uma forma anteriormente inimaginável (MENDES, 2014, p. 27).

Os pioneiros nessa temática foram Warren e Brandeis, que por meio do artigo “The right to privacy”, denunciavam como aparatos tecnológicos dentre outros, tinham invadido os sagrados domínios da vida privada e doméstica (WARREN, Samuel; BRANDEIS, Louis 1890 apud MENDES, 2014, p. 27).

Foram estes autores que quebraram o entendimento anterior que associava a proteção da vida privada à propriedade, trazendo uma nova associação à inviolabilidade da personalidade.

Conforme delineado por Mendes (2014, p. 29):

> No decorrer do século XX, a transformação da função do Estado, aliada à revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. De um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático. É nesse sentido que se pode afirmar que o século passado vivenciou um “processo de inexorável reinvenção da privacidade”.

Quando se diz de um direito negativo, está se referindo à abstenção do Estado de interferir na esfera privada do indivíduo para garantia de tal direito. Houve

uma mudança para um direito positivo ativo, de não interferir para interferir e proteger, transformando-se posteriormente nos indícios da proteção dos dados pessoais.

A mudança nesse conceito, refletiu diretamente nas legislações específicas e decisões judiciais de diversos países, em que estes instrumentos passaram a compartilhar do conceito de que os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela jurídica (MENDES, 2014, p. 29).

Segundo a ótima reflexão de MENDES (2014, p.32):

> (...) a partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais. Nesse contexto, percebe-se uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominada privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros. Dessa forma, opera-se na dogmática e na prática jurídica uma clara evolução no direito à privacidade.

Desse modo, percebe-se que a proteção de dados pessoais se origina da proteção à inviolabilidade da personalidade por meio do direito positivo à privacidade. Em que quando se salvaguarda um, em cadeia, salvaguarda outro.

4.2 O Direito Fundamental à Proteção de Dados Pessoais

Imperioso ressaltar, conforme dito no início deste trabalho, com a globalização, os aspectos sociais, econômicos, culturais, também acompanharam essa evolução, na verdade constituem essa evolução. O mesmo aconteceu com a proteção de dados, em que, com uma interpretação sistemática da CRFB de 1988, pode-se identificar como um direito fundamental a proteção aos dados pessoais na Lei Maior.

Essa proteção é identificada como uma dimensão da inviolabilidade da intimidade e da vida privada, nos termos da Constituição, conforme Laura Schertel Mendes (2014, p.171). Sendo importante citar a douta análise dessa doutrinadora:

> A partir do art. 5º, X, da CF, que garante a inviolabilidade da intimidade e da vida privada, é possível extrair uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele

> se encontra. Não faria sentido excluir exatamente as situações em que a sua vida privada está sujeita a uma maior violação, como é o caso do processamento de dados pessoais. Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos “tradicionais”, que ensejaram o nascimento desse direito, como a hipótese de ser flagrado por paparazzi ou de ser notícia de jornais sensacionalistas. Assim, se não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos.

Diante disso, como a Carta Magna tem flexibilidade temporal, como é o caso das mutações constitucionais, é totalmente viável a aceitabilidade da proteção de dados como um direito fundamental, pois é um problema emergente e que precisa de amparo de lei com a força da Constituição.

Ademais, não faz sentido negar que é fundamental a proteção de dados quando a Constituição tutela direitos semelhantes. Acontece que os fatos mudaram, cabendo a legislação, como é para acontecer, acompanhar essa mudança. No final, continua sendo o objetivo, a proteção a privacidade, e a inviolabilidade da personalidade.

4.3 Proteção de dados pessoais e o Direito do Consumidor

O Direito do Consumidor pode ser definido como o conjunto de princípios e regras destinados à proteção do consumidor (CAVALIERI FILHO, 2019).

O próprio Código de Defesa do Consumidor, em seu artigo 2º, define o consumidor como “toda pessoa física ou jurídica que adquire ou utiliza produto como destinatário final”.

No mesmo código foi criada a Política Nacional de Relações de Consumo, que “tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo”, atendendo diversos princípios.

Diante dessas breves explanações, dá para perceber que, além de outros ordenamentos pátrios que já protegem o indivíduo em si, há um sistema voltado diretamente para o consumidor, abarcando diversos aspectos de sua vida,

demonstrando inclusive, sua vulnerabilidade frente aos fornecedores e prestadores de serviço.

Conforme interpretação realizada da Constituição Federal, que demonstrou o cabimento da proteção de dados pessoais como um direito fundamental, o mesmo acontece no Direito do Consumidor, em que por ser também um código aberto a interpretações, é possível também extrair o entendimento de direito básico do consumidor à proteção de dados pessoais.

Isso envolve uma dupla dimensão de acordo Laura Schertel Mendes (2014, p. 203):

> (...) (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.

Essas duas dimensões são fundamentais pois possibilitam a autodeterminação informativa do consumidor, como ao mesmo tempo propicia um controle objetivo de legitimidade do tratamento de dados pessoais (MENDES, 2014, p. 203).

A autodeterminação informativa tem como objetivo o consumidor ter controle sob os seus dados, de deixar ser exposto somente o que ele deseja, protegendo a sua personalidade contra os diversos riscos oriundos da exposição desenfreada dos dados pessoais.

Em relação ao controle do fluxo desses dados, é justamente ter o poder de cessar a fonte de informação quando quiser, ou até de modificar dados que possivelmente não transmitam a realidade.

Em suma, o consumidor está protegido no que se trata da sua personalidade, conforme demonstrado, e isso incluem os seus dados que são uma projeção digital da sua vida real, pelo Código de Defesa do Consumidor, pois se há proteção da personalidade, e os dados são uma projeção desta, consequentemente os dados estão tutelados pelo código.

No entanto, para além dessa interpretação extensiva, é importante os países terem legislações específicas que tratem da temática, e isso verificaremos a seguir.

4.3 Princípios da proteção de dados pessoais

Antes de se adentrar de fato em algumas legislações específicas acerca da proteção de dados pessoais, é necessário discorrer sobre princípios que regem a temática.

Tomando como base vários ordenamentos, pode se verificar uma convergência nas soluções legislativas sobre a matéria em diversos países, como também uma tendência rumo à consolidação de princípios básicos (DONEDA, 2010, p.43).

A origem da discussão do núcleo básico desses princípios tem origem na década de 1960, durante tentativa falha de criação de gigantesco banco de dados com uma série de informações sobre os cidadãos norte-americanos, a fim de utilização na administração pública.

Mesmo após fracasso do estabelecimento desse banco de dados, vários temas sobre a possibilidade de sua criação, continuaram a ser desenvolvidos. Até que no início da década de 1970, a *Secretary for Health, Education and Welfare (HEW)* – secretária do governo estadunidense – reuniu uma comissão de especialista da área que desenvolveram um estudo que concluiu pela relação entre a privacidade e os tratamentos de dados pessoais, e pela necessidade de estabelecer a regra do controle sobre as próprias informações (DONEDA, 2010, p.44).

As regras desenvolvidas por esse estudo se tornaram as chamadas *Fair Information Principles*, passando inclusive a serem encontradas nos mais diversos ordenamentos que tratem sobre proteção de dados. Tornando assim, base para qualquer legislação nesta seara.

Agora de fato, trazendo estes princípios, os são apresentados com breve descrição do doutrinador Danilo Doneda (2010, p.46), que tomou como base a enunciação do *Department of Homeland* – Departamento de Segurança Interna - *Security* norte-americano no ano de 2008:

> 1 - *Princípio da transparência*, pelo qual o tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento.
> 2 - *Princípio da qualidade*, pelo qual os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam

> feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade.
> 3 - *Princípio da finalidade*, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).
> 4 - *Princípio do livre acesso*, pelo qual o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros; após este acesso e de acordo com o princípio da qualidade, as informações incorretas poderão ser corrigidas, aquelas registradas indevidamente poderão ser canceladas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos.
> 5 - *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Apesar de indubitavelmente bem explanado por Danilo Doneda (2010, p.46), importante realizar alguns apontamentos sobre estes princípios.

O Princípio da Transparência, também pode ser chamado de princípio da publicidade, como o próprio nome indica, impõe que se deve manter a clareza acerca do armazenamento e tratamento de dados, em que os bancos de dados sejam de conhecimento público, afinal, os usuários tendo ciência de que seus dados estão sob a tutela de um terceiro, fica mais fácil de agir diante de irregularidades.

Diante desse princípio, surge para os bancos de dados realizarem registros públicos, publicando seu nome, sede e conteúdo, inclusive em meios grandes de circulação. Em alguns países é necessário até prévia autorização estatal ou notificação ao órgão supervisor, como um pressuposto para o funcionamento dos bancos de dados (MENDES, 2014, p.71).

O Princípio da Qualidade visa tornar os dados armazenados os mais fiéis possíveis à realidade, e que o processamento não seja realizado de qualquer forma. De acordo com MENDES (2014, p.72), para “a efetividade do princípio da qualidade de dados, é fundamental a garantia dos *direitos de acesso, retificação e cancelamento dos dados.*”, ou seja, é necessário que a fidelidade das informações sejam a todo tempo, podendo o usuário atualizá-las e apagá-las quando desejar.

O Princípio da Finalidade é aquele responsável por proteger a forma de utilização dos dados. Ora, conforme delineado, as informações pessoais podem ser

utilizadas das mais diversas formas, desse modo é necessário que se defina exatamente para que certos dados serão usados, qual o fim almejado, para que não haja abusividades. Então esse princípio vincula a forma como dados são usados à comunicação aos fornecedores.

Esse princípio é necessário para se limitar o acesso de terceiros ao banco de dados, como também serve de parâmetro para determinar se o uso de dados pessoais processados é adequado e razoável de acordo com a finalidade informada ao interessado (MENDES, 2014, p.70).

Há inclusive jurisprudência referente a esse princípio, do Tribunal de Justiça do Estado de São Paulo, que reconheceu em um caso o princípio da finalidade, no qual uma empresa fez um repasse de dados cadastrais sem autorização do titular. O consumidor realizou um cadastro numa loja de departamentos, e descobriu que tais dados foram repassados indevidamente à mãe de filha, sendo utilizados para embasar uma ação de alimentos contra ele. Ante isso o consumidor ajuizou ação indenizatória contra a empresa, alegando danos morais pela violação da privacidade. Em primeira instância teve seu pedido julgado procedente, fixada indenização em dez salários mínimos, e mesmo após recurso da parte contrária a condenação foi mantida (MENDES, 2014, p. 137).

Veja-se a ementa do acordão:

> RESPONSABILIDADE CIVIL – Ação de indenização por danos morais – Cerceamento de defesa – Inocorrência – Ré que repassou dados cadastrais acerca dos rendimentos do autor a terceira estranha e com fins sem qualquer ligação a outra relação de consumo – Abuso do objeto cadastral em detrimento da privacidade do autor – Dano moral in re ipsa – Quantum que não merece reparo – Correção monetária, por outro lado, que deve incidir a partir da data em que o valor foi arbitrado – Incidência de juros mantida a partir da cita- ção – Encargos da sucumbência – Reciprocidade – Inocorrência – Gratuidade processual que não pode ser revogada com base em futura indenização – Litigância de má-fé – Inocorrência – Recurso provido em parte.
> (TJSP, Apelação Cível 355.607.4/0-00, Relator Desembargador De Santi Ribeiro, 2-7-2009)

Aqui ser percebe uma forte jurisprudência acerca de um dos princípios da proteção de dados pessoais, em que foi determinada em 1º grau, e consolidado em 2º grau, o que dispõe o princípio da finalidade.

Continuando, tem-se o Princípio do Livre Acesso como também o próprio nome já acusa, traz a ideia de que as pessoas devem ter total acesso aos seus dados a qualquer momento, a fim de averiguação e em conjunto com o Princípio da Qualidade, realizar modificações caso necessário.

Importante ressaltar que no ordenamento brasileiro há uma ação específica para esses casos, chamada *Habeas Data*.

E por último, o Princípio da Segurança Física e Lógica, princípio este importantíssimo, pois conforme demonstrado, um dos problemas do armazenamento de dados é justamente a possibilidade de vazamento, que pode ter como consequência a utilização indevida dos dados. Sendo assim, é necessário a criação de métodos de proteção a fim de evitar extravios e utilização não autorizadas pelos interessados.

4.4 GDPR – *General Data Protection Regulation* (Regulamento 2016/679 da União Europeia)

Agora partindo de fato para as legislações específicas existentes, a análise se inicia pela GDPR – *General Data Protection Regulation* – que é a lei de maior relevância internacional no que concerne à proteção de dados, sendo referência em todo o mundo. Em tradução livre significa Regulamento Geral de Proteção de Dados.

Este conhecido ordenamento foi originado em forma de regulamento, o 2016/679 da União Europeia. Desse modo, inicialmente é importante trazer a natureza jurídica desse tipo de norma.

Os Regulamentos são normas vinculativas aplicadas diretamente a todos os países integrantes da União Europeia, incluindo os cidadãos e as pessoas jurídicas, valendo como se fosse o direito de cada país. Diretivas são normas adotadas pela Comissão e pelo Parlamento Europeu, sendo tipo objetivos a serem atingidos por todos os Estados-Membros (GUIDI, 2018, p.87).

Apesar da GDPR ter sido regulamentada recentemente, o sistema europeu de proteção de dados pessoais era regido por diversas diretivas, tendo como texto legal central a Diretiva 95/46/CE, que centraliza os principais conceitos no campo da proteção de dados pessoas na União Europeia, trazendo princípios básicos tanto na coleta, quanto na manipulação e tratamento de tais dados pelos interessados e por

terceiros, como também direitos básicos dos titulares, entre outros (GUIDI, 2018, p. 91-92).

A GDPR veio para consolidar, reafirmar e constituir novos direitos relativos a proteção de dados pessoais. Cita-se as observações de Guilherme Berti de Campos Guidi (2018, p.92):

> Entre as principais alterações trazidas pela GDPR, pode-se apontar algumas que são mais relevantes e que podem ser divididas por sua finalidade: alterações para reforçar os direitos dos usuários, alterações para reforçar as competências das Autoridades de Proteção de Dados, e alterações para induzir e incentivas certos comportamentos por parte dos responsáveis pelo tratamento.

As alterações trazidas pela GDPR foram necessárias para dar uma força maior aos diversos dispositivos dos regulamentos, tudo voltado para uma melhor proteção do titular dos dados.

Feitas essas elucidações, agora se traz pontos relevantes da GDPR que merecem ser citadas. Será visto que, os princípios que regem a proteção de dados por diversos ordenamentos, são consolidados nos artigos do corpo da GDPR.

Inicialmente a GDPR traz diversas considerações, que vão desde a consolidação de que a proteção dos dados pessoais é um direito fundamental, passando pelo objetivo do referido ordenamento, explicações pertinentes à temática, o porquê de se proteger os dados, até procedimentos e responsabilidades das autoridades. Não deixando de ser uma breve explanação do conteúdo do corpo do regulamento.

Apesar de não ser extensa, possuindo apenas 99 artigos, se focará para este trabalho em pontos que merecem maior destaque, utilizando-se do texto de Ronaldo Gogoni (2018), do site meiobit.com, que elencou regras da GDPR que colocam o usuário como soberano de seus dados. Veja-se:

- o usuário é soberano no direito de autorizar ou não a coleta de dados, e tem o direito de determinar como eles serão tratados;
- o usuário tem o direito de saber quais dados uma determinada empresa está coletando e para quais fins;
- o usuário tem o direito de mudar de opinião quando quiser, sendo as empresas obrigadas a fornecer ferramentas para remoção de dados e sua decisão de interromper a coleta deve ser respeitada;
- o usuário tem o direito de ser informado se seus dados estão sendo compartilhados com empresas ou grupos externos;

- o usuário tem o direito à portabilidade de dados, de modo que ele possa baixa-los e disponibiliza-los em outro serviço ou à sua escolha, e as empresas são obrigadas a fornecer ferramentas para tal finalidade;
- o usuário tem o direito de apagar seus dados em ocasiões específicas;
- as empresas ficam obrigadas a notificar os usuários e as autoridades em até 72 horas após uma ocorrência de vazamento de dados;
- as empresas são obrigadas a considerar a proteção de dados e privacidade dos usuários por design, desde o início de qualquer projeto;
- as empresas são obrigadas, na medida do possível aplicar a pseudoanonimação dos dados, de modo a dificultar a identificação das informações por terceiros; a GDPR menciona métodos de ocultação e/ou substituição de dados de forma que a identificação correta só possa ser realizada com a adição de mais dados;
- as empresas são obrigadas a manter registros internos de todas as atividades de processamento dos dados dos usuários, e elas deverão incluir nome e detalhes da organização, a finalidade do processamento, a descrição de categorias de indivíduos e dados pessoais, destinatários, detalhes da transferência e cronogramas de retenção de dados;
- as empresas ficam proibidas de transferir dados para um país que não possua leis adequadas de proteção aos dados; a Comissão Europeia manterá uma lista de "países aprovados" para as transações e de forma alguma os inclusos na "lista negra" deverão ter acesso a informações de cidadãos europeus;
- fornecedores terceirizados estão sujeitos às mesmas regras; basicamente, qualquer companhia que lide com dados de europeus será obrigada a manter registros de suas atividades, mesmo que sirva apenas como uma intermediária;
- as empresas deverão nomear um Diretor de Proteção de Dados (Data Protection Officer, ou DPO), um executivo responsável pela supervisão da manutenção e tratamento dos dados, que também deverá atuar como elo de ligação com as autoridades para prestar esclarecimentos e auxiliar em investigações.

Ante as garantias consolidadas pela regulamentação europeia, se verifica o quanto os usuários passaram a ter controle sobre os seus dados, pelos menos legalmente, e como foi dado atenção legislativa a esse tipo de temática.

Direitos como autorizar ou não a coleta de dados, apagar quando quiser, finalidade, notificação ao titular sobre vazamento, aplicação de pseudoanonimação, registro por parte das empresas que estão realizando o processamento e armazenamento, são direitos basilares e refletem o quanto o direito de proteção de dados cresceu, e vem ganhando seu devido espaço nas legislações de diversos países.

Percebe-se que diversos direitos acerca da proteção de dados são garantidos aos usuários. Ótimo sinal, tendo em vista a importância de proteção desse tipo de informação. Também se percebe, consoante dito, que os direitos garantidos nesse regulamento, seguem os princípios concernentes à proteção de dados. E como se verá no próximo tópico, a LGPD – Lei Geral de Proteção de Dados, que é o ordenamento brasileiro nesta seara, se baseou em muito nos princípios e no regulamento europeu.

4.5 LGPD – Lei Geral de Proteção de Dados (Lei n.º 13.709/2018)

Agora se parte para análise de um dos dispositivos da legislação brasileira no que concerne à proteção de dados.

A Lei Geral de Proteção de Dados, também conhecida pela sigla LGPD, de n.º 13.709/2018, foi promulgada pelo presidente Michel Temer em 14 de agosto de 2018, com vigência integral dois anos depois. Foi originária do Projeto de Lei Complementar n.º 53/2018 de iniciativa do Deputado Federal Milton Monti.

Inicialmente é imperioso citar as considerações iniciais da Doutora Patríci Peck Pinheiro (2018) acerca da LGPD:

> A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas.

Conforme já demonstrado ao longo deste trabalho, a proteção aos dados pessoais, interfere diretamente no direito da personalidade do indivíduo, e consequentemente no direito à privacidade. Desse modo, ficou o claro o quanto é essencial uma legislação específica para proteger um bem tão precioso. E assim o Brasil o fez, com a instituição da Lei Geral de Proteção de Dados, demonstrou claramente que a tutela desses direitos tem importância no país.

A LGPD é composta por 65 artigos, distribuídos em 10 capítulos, dispostos da seguinte maneira:

• Capítulo I – Disposições Preliminares (arts. 1° ao 6°);

• Capítulo II – Do Tratamento de Dados Pessoais (arts. 7° ao 16): há Seção I (Dos Requisitos para o Tratamento dos Dados), Seção II (Do Tratamento de Dados Pessoais Sensíveis), Seção III (Do Tratamento de Dados Pessoais de Crianças e Adolescentes) e Seção IV (Do Término do Tratamento de Dados);

• Capítulo III – Dos Direitos do Titular (arts. 17 ao 22);

• Capítulo IV – Do Tratamento de Dados Pessoais pelo Poder Público (arts. 23 ao 32): contém Seção I (Das Regras) e Seção II (Da Responsabilidade);

• Capítulo V – Da Transferência Internacional de Dados (arts. 33 ao 36);

• Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais (arts. 37 ao 45): contém Seção I (Do Controlador e do Operador), Seção II (Do Encarregado pelo Tratamento de Dados Pessoais) e Seção III (Da Responsabilidade e do Ressarcimento de Danos).

• Capítulo VII – Da Segurança e das Boas Práticas (arts. 46 ao 51): contém Seção I (Da Segurança e do Sigilo de Dados) e Seção II (Das Boas Práticas e da Governança).

• Capítulo VIII – Da Fiscalização (arts. 52 ao 54): contém Seção I (Das Sanções Administrativas).

• Capítulo IX – Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (arts. 55 ao 59): contém Seção I (Da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Seção II (Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade) – veto presidencial.

• Capítulo X – Disposições Finais e Transitórias (arts. 60 ao 65).

Diante disso, percebe-se certa semelhança na disposição dos temas tratados, com a GDPR. Iniciando com disposições preliminares, passando por conceitos, até autoridades da área. Essa semelhança, é justamente por a LGPD ter também como base os princípios gerais da proteção de dados e a própria GDPR.

Como igualmente feito no tópico que foi tratado sobre a GDPR, se faz necessário destacar os pontos mais relevantes da LGPD, no entanto, fica o registro que toda essa lei é de suma importância para as pessoas em geral.

Inicialmente é essencial trazer a que a lei é aplicada, e conforme o artigo 3º, se aplica em qualquer operação de tratamento de dados, seja realizada por pessoa

natural ou jurídica, do país de sua sede ou do país em que estejam os dados. No entanto, é necessário que o tratamento ou a coleta dos dados sejam realizados no território nacional, ou ainda que a atividade de tratamento tenha por objetivo o fornecimento de bens e serviços, independentemente do país que o tratamento ocorra. O que se verifica, é que felizmente a lei abarca qualquer tratamento de dados, que se utilize de dados extraídos dos usuários brasileiros no Brasil. Então independe que o prestador de serviço seja nacional ou estrangeiro, se captar dados no Brasil, estará sob a tutela da LGPD.

Ilustrando, a Netflix que é empresa norte-americana, mas que possui diversos clientes no Brasil, consequentemente, também possui grande número de dados dos brasileiros, sendo assim está totalmente regida pela LGPD.

Além dos princípios gerais acerca da proteção de dados apresentados, a lei brasileira traz outros princípios de conteúdo semelhante e outros que desmiuçam ainda mais aqueles, que é o caso dos princípios da Adequação, Necessidade, Prevenção e Não Discriminação.

O Princípio da Adequação, conforme o texto da lei, impõe que o tratamento realizado seja compatível com as finalidades informadas ao titular dos dados. O da Necessidade por sua vez, determina que o tratamento seja o mínimo possível, para atingir a finalidade buscada. O da Prevenção está intimamente ligado ao Princípio da Segurança Física e Lógica, pois é um método de segurança a adoção de medidas a fim de evitar a ocorrência de dados em virtude do tratamento. E por fim, o Princípio da Não Discriminação, que visa a não discriminação oriunda do tratamento de dados.

Seguindo com destaques da LGPD, imperioso ressaltar quais são as situações que o tratamento de dados é considerado legal, e isto está disposto inicialmente entre os artigos 7º e 16º. Foi levado em conta os requisitos, as hipóteses de tratamento, o tratamento de dados pessoas de crianças e adolescente e o término do tratamento de dados.

As hipóteses legais para o tratamento legítimo dos dados pessoais, estão bem destrinchados na LGPD. Veja-se:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Umas das palavras-chaves para tratamento de dados estar dentro da legalidade é “consentimento”. Com a lei em vigor, é necessário que os titulares dos dados tenham autorizado o processamento dos mesmos, sendo este a disposição do inciso I do artigo 7º. E o artigo 8º da mesma lei, reforça isso, determinando que o consentimento seja por escrito, ou por um outro meio que de fato, demonstre a manifestação de vontade do titular.

No que concerne ao tratamento de dados pessoais sensíveis, o rol bem menor, mas ainda exige o consentimento do titular.

Em relação ao tratamento dos dados pessoais das crianças e adolescentes, a questão do consentimento continua, mas nesse é realizado por um dos pais ou responsáveis, sendo dispensado somente nos casos de coleta visando contato com os pais ou responsável legal.

De acordo com a lei, o tratamento de dados deve finalizar quando tiver sua finalidade alcançada de acordo com o consentimento dado, seja o fim do período de tratamento, ou o próprio titular revogue o consentimento, ou ainda por determinação da autoridade nacional em caso de violação do disposto na LGPD.

Em relação aos direitos dos titulares dos dados, é basicamente o trazido em alguns dos princípios apresentados, mas vale trazer também a literalidade da lei:

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Vê-se que a lei traz grande proteção ao titular, e lhe concede grande poder, tanto de verificação, modificação e revogação dos dados que lhe concernem. Esse artigo é mais um apoio do direito de dar consentimento ou não, pois caso os dados não estejam conforme o titular almeja, ou este não tenha mais interesse em fornecê-lo, pode a qualquer momento modificá-lo ou revogá-lo.

Um outro ponto que merece destaque é acerca da fiscalização do cumprimento da LGPD.

Conforme determinado pela lei, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, que tem dentre outras competências, zelar pela proteção dos dados pessoais, fiscalizar e aplicar sanções em caso de descumprimento da legislação pertinente e promover na população o conhecimento das normas e políticas públicas sobre a proteção de dados pessoais.

Dentre as sanções administrativas, que são aplicáveis pela autoridade nacional, aqui se destaca a advertência, onde deverá ser indicado prazo para realizar medidas corretivas; multa simples de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado; multa diária; publicização da infração, após apuração e confirmação de sua ocorrência; bloqueio dos dados pessoais; e eliminação dos dados pessoais a que se refere a infração.

Diante dessas explanações, o que se observa é que deveras a lei trouxe um belo subsídio legal para os titulares de dados, como também aval legal para as empresas utilizarem os dados pessoais de terceiros, desde que observado as pertinências da lei. Pois não sendo assim, estarão, os agentes de tratamento de dados, sujeitos às sanções da Lei Geral de Proteção de Dados, fiscalizada pelo órgão criado para esse e outros fins.

Desse modo, verifica-se que de fato o sistema jurídico brasileiro salvaguarda os dados pessoais, incluindo o dos consumidores. Apesar de ainda estar para entrar em vigência uma lei de grande importância que é a LGPD, a legislação existente já tem base para proteger os dados pessoais, como é o caso da Constituição Federal de 1988, que já torna fundamental o direito de personalidade que como foi visto, abarca a proteção dos dados pessoais por meio do direito à privacidade. Uma outra legislação é o Código de Defesa do Consumidor, por meio da tutela da personalidade do consumidor, como também a garantia de controlar o seu fluxo de dados.

Contudo é a Lei Geral de Proteção de Dados, que sendo mais específica vem para codificar e reafirmar os direitos da proteção de dados no Brasil, com diversos dispositivos garantidores desse direito. No entanto, é preciso manter atenção sobre a sua aplicação, para que de fato as medidas sejam efetivas, e que os órgãos criados pela lei, ajam de acordo com o que ela prega e dispõe, em seus princípios e artigos. Mas além do órgão em específico, é necessário que a sociedade em geral, titular dos dados, fiscalizem a real aplicação e que sempre que puder e for necessário, recorram ao Poder Judiciário para reafirma os direitos tabulados na legislação.

5 CONSIDERAÇÕES FINAIS

O presente trabalho objetivou analisar as questões pertinentes à proteção de dados pessoais, desde os perigos inerente, até as legislações aplicáveis. Teve como objeto maior verificar se de fato, no Brasil, os dados pessoais estão salvaguardados pela legislação, se há efetivas medidas de proteção.

Nesse sentido, consoante demonstrado no primeiro capítulo, diversos conceitos necessários à boa compreensão do trabalho foram apresentados. Por ser uma área envolvida com tecnologia, é importante deixar o leitor por dentro dos novos mecanismos utilizados para captação e utilização dos dados. Desse modo, foi trazido desde conceitos simples, como o de dados, até mecanismos mais complexos como *Big Data* e *Cookies.*

No segundo capítulo, foram apresentados os perigos e problemas inerentes à captação, processamento e armazenamento de dados. Em que restou comprovado que estes podem ser utilizados das mais diversas formas possíveis, sendo este um dos motivos para protegê-los. Foram colocados como exemplos o direcionamento de publicidade, o vazamento de dados em massa, entre outros. Aqui demonstrou-se a necessidade de proteger os dados, origem do problema do presente trabalho: os perigos que rodeiam os dados pessoais.

E por fim, no terceiro capítulo, foi realizada uma breve análise acerca das legislações aplicadas no que concerne à proteção de dados, incluindo princípios e leis pertinentes. Onde verificou-se que legalmente há providências, restando verificar se estas serão respeitadas ao longo do tempo. Ou seja, foi apresentada a hipótese de que os dados pessoais estão no Brasil, legalmente protegidos, mas que é necessário a continua fiscalização, tanto por parte dos titulares dos dados, como também pelo poder público.

Diante todas as exposições realizadas, verifica-se a grande importância que é de se proteger os dados pessoais. Ora, com a evolução do mundo, e das relações interpessoais, novos problemas surgiram, e que não são simples. Diante disso, se faz necessário que novos meios de proteção as pessoas sejam instituídos, como é o caso da Lei Geral de Proteção de Dados.

Conforme demonstrado, os perigos são diversos e graves, que mexem intimamente com o ser humano, podendo influir até no seu poder de escolha, ou

mesmo pelo “simples” fato de divulgação de diversos dos seus dados sem autorização.

No entanto, percebeu-se que os países vêm dando a atenção que essa temática merece. Criando legislações e autoridades para proteger os dados pessoais, conforme demonstrado a instituição dos princípios gerais, da GDPR, e da LGPD. Como também, ordenamentos existentes antes mesmo desse tipo de discussão vir à tona, abrir margem de interpretação a fim de favorecer a proteção dos dados, como é o caso da CRFB/88, e o Código de Defesa do Consumidor.

Enfim, felizmente novos passos foram dados, sendo assim, tendo vista a Proteção de Dados Pessoais ser um direito fundamental, ou seja, de grande força, não pode de maneira alguma regredir.

Agora, o que resta é ficar atento se de fato todos os direitos determinados nas legislações serão respeitados, cabendo ao órgão criado, e até os titulares dos direitos, fiscalizarem o cumprimento da legislação, a fim de que os dados pessoais de todos estejam protegidos.

REFERÊNCIAS

ALVES, Paulo. O que são cookies? Entenda os dados que os sites guardam sobre você. **Techtudo**, 04 de out. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml. Acesso em: 27 dez. de 2019.

BIONI, Ricardo, B. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. 2nd edição. Rio de Janeiro: Forense, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530988777/cfi/6/2!/4/2/2@0:0 Acesso em 10 de dez. de 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em: 20 de dez. de 2019.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em 21 de dez. de 2019.

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**.
Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em 14 de janeiro de 2020.

BBC NEWS. Entenda o escândalo de uso político e dados que derrubou valor do Facebook e o colocou na mira de autoridades. **G1**. 20 de mar. de 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml - Acesso em: 20 de jan. de 2020.

CASAROTTO, Camila. Saiba o que é Publicidade, para que serve e como é a carreira do publicitário. **Rock Content**, 05 de fev. 2019. Disponível em: https://rockcontent.com/blog/publicidade/ Acesso em: 14 de jan. de 2020.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005.

CAVALIERI FILHO, Sérgio. **Programa de direito do consumidor**. 5ª edição. São Paulo: Atlas, 2019.

ÉPOCA NEGÓCIOS ONLINE. Facebook escuta e transcreve conversas de áudio do Messenger. **Época Negócios**. 14 de ago. de 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/08/facebook-escuta-e-transcreve-conversas-de-audio-do-messenger.html - Acesso em: 20 de janeiro de 2020.

EUROPA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Regulamento Geral sobre a Proteção de Dados**. Disponível em: https://eurex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em 12 de dez. de 2019.

DE CASTRO, Leandro Nunes; FERRARI, Daniel Gomes**. Introdução à mineração de dados: conceitos básicos, algoritmos e aplicação** / Leandro Nunes de Castro, Daniel Gomes Ferrari. 1ª edição. São Paulo: Saraiva, 2016. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/978-85-472-0100-5/cfi/0!/4/2@100:0.00 Acesso em 10 de jan. de 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia** / Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010.

GOGONI, Ronaldo. O que é o GDPR e por que ele vai afetar a vida de todos nós. **Meio Bit**. 2018. Disponível em: https://meiobit.com/385028/gdpr-novo-regulamento-privacidade-dados-uniao-europeia-o-que-e/ - Acesso em: 05 de fev. de 2020.

GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais – Privacidade em Perspectivas** / organizadores Sérgio Branco, Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

HRON, Martin. Os últimos 10 maiores vazamentos de dados. **Avast Blog**. 14 de fev. de 2019. Disponível em: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados - Acesso em: 20 de janeiro de 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor : linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. (Série IDP : linha pesquisa acadêmica) Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502218987/cfi/0. Acesso em 10 de dez. de 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13709/2018 (LGPD)**. 2ª edição. São Paulo: Saraiva Educação, 2020.

SETZER, Valdemar W; SILVA, Flávio Soares Corrêa da. **Banco de Dados: aprenda o que são, melhore seu conhecimento, construa os seus**. 1ª edição. São Paulo: Blucher, 2005. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788521216520/cfi/0!/4/2@100:0.00 Acesso em 10 de jan. de 2020.

Tribunal de Justiça de São Paulo, **Apelação Cível n.º 355.607.4/0-00**, Relator Desembargador De Santi Ribeiro, 02 de jul. 2009.