



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS  
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS  
NÚCLEO DE PRÁTICA JURÍDICA  
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO  
ARTIGO CIENTÍFICO

**A PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE VIRTUAL  
E A  
LEGISLAÇÃO BRASILEIRA**

ORIENTANDO (A): Frederico  
ORIENTADOR (A): PROF. MA. Tatiana

GOIÂNIA

2020

Frederico Queiroz Rebouças

**A PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE VIRTUAL  
E A  
LEGISLAÇÃO BRASILEIRA**

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof.<sup>a</sup> Orientadora: MA. Tatiana de Oliveira Takeda

GOIÂNIA  
2020  
FREDERICO QUEIROZ REBOUÇAS

**A PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE VIRTUAL  
E A  
LEGISLAÇÃO BRASILEIRA**

Data da Defesa: \_\_\_\_ de \_\_\_\_\_ de 2020.

BANCA EXAMINADORA

---

Orientador: Prof. Titulação e Nome Completo

Nota

---

Examinador Convidado: Prof. Titulação e Nome Completo

Nota

Dedicatória

Agradecimento

# SUMÁRIO

<b>RESUMO/ABSTRACT .....</b>	
<b>INTRODUÇÃO .....</b>	
<b>SEÇÃO 1 - DOS DADOS E SEU HISTÓRICO</b>	
1.1 - DO HISTÓRICO DOS DADOS PESSOAIS	
1.2 - DO MARCO CIVIL DA INTERNET	
1.3 - DOS DADOS PESSOAIS	
1.3.1 - Dos Dados Sensíveis	
1.3.2 - Dos Dados Anônimos	
<b>SEÇÃO 2 - DA LEGISLAÇÃO BRASILEIRA</b>	
2.1 - DA INSTAURAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA - LGPD	
2.2 - DA LEI GERAL DE PROTEÇÃO DE DADOS	
2.3 - DOS PRINCÍPIOS DOS DADOS PESSOAIS	
2.4 - DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS	
<b>SEÇÃO 3 - DOS DADOS E A PRIVACIDADE</b>	
3.1 – DO USO DOS DADOS	
3.2 - DA PRIVACIDADE	
<b>CONSIDERAÇÕES FINAIS.....</b>	
<b>REFERÊNCIAS .....</b>	

## RESUMO

O resumo em língua vernácula é obrigatório. O texto do resumo deve ser justificado, fonte ARIAL 12, contendo entre 100 e 250 palavras, em parágrafo único, sem recuo, com entrelinhamento simples. Concluído o texto, sem saltar linhas, seguem as palavras-chave ou descritores. O tempo verbal é passado.

**Palavras-chave: Entre três e cinco.**

## ABSTRACT

O resumo em língua estrangeira.

**Key-words:.**

# **A PROTEÇÃO DE DADOS PESSOAIS NO AMBIENTE VIRTUAL E A LEGISLAÇÃO BRASILEIRA**

Frederico Queiroz Rebouças

## **INTRODUÇÃO**

Este trabalho vem em razão da cominação de anos de especulação e um olhar observador sobre a maneira que progredimos no sentido de compartilhar nossas vidas com o mundo através da *Internet*, este é oriundo de um desejo de compreender mais profundamente da forma como é tratado algo tão valioso para todo nós, nossa própria informação e tudo que produzimos enquanto conectados.

O estudo dos dados e sua compreensão traz consigo uma infinidade de problemas causados pelos mesmos, variando de uma má gestão por parte tanto do controlador como do titular até a geração de consequências que poderiam transformar completamente o rumo da humanidade e alterar a forma como se vive em sociedade, podendo isto variar tanto para o bem como para o mal, dependendo da forma como é tratado.

Ciente da enorme problemática que envolve todo este assunto, este projeto almeja trazer informações importantes para o conhecimento de todos, buscando assim trazer ao maior número de pessoas possíveis, informações sobre como foi, como é e como possivelmente será o tratamento dos dados oriundos da população, conhecimento este que é de vital importância no que tange a proteção da privacidade individual e coletiva.

A Seção 1 discorre acerca da evolução histórica que os dados passaram, se transformando completamente nessa caminhada, traz também sobre os primórdios da legislação referente no Brasil assim como terminologia de vital importância para se compreender o restante da pesquisa.

Na Seção seguinte, se encontra informações a respeito da nova legislação brasileira sobre o assunto, a Lei Geral de Proteção de Dados (LGPD) junto de uma tentativa de sintetizar e explicar as consequências e razões advindas dos pontos mais importantes da lei, buscando trazer a informação com clareza.

Em sua última Seção, encontram-se aprofundados exemplos de casos que constantemente fogem ao olhar do espectador desinformado, casos e situações únicas que nasceram do avanço da tecnologia no mundo moderno, em sua essência é um texto informativo que procura da melhor forma possível desconstruir as relações nascidas desta era dos dados que nos cerca e tão rasamente se compreende.

## **SEÇÃO 1**

### **DOS DADOS E SEU HISTÓRICO**

#### **1.1 - DO HISTÓRICO DOS DADOS PESSOAIS**

Dados pessoais são todos aqueles que se acumulam de ocorrências e fatos que um indivíduo coleta durante a vida, definindo sua personalidade e esse acumulado de informações podem prover de forma precisa, mais do que imaginamos, a vida e a história de cada indivíduo. Ao decorrer da História da Humanidade, essas informações vieram em vários tipos de formatos, diários, telegramas, documentos pessoais, cartas, livros, fotos e com o advento da internet, esse rol de formatos se expandiu exponencialmente, sendo possível adquirir informações sobre alguém através do seu histórico de acesso, redes sociais e blogs. Nota-se também que inclusive o governo faz uso de tais formações para manter controle sobre seus cidadãos, utilizando de bancos de dados virtuais, guardando todo tipo de informações sobre cada indivíduo, sendo alguns exemplos o Certificado de Pessoa Física e o Imposto de Renda.

A sociedade nos tempos atuais já se encontra lidando com a realidade da identificação biométrica, modelo este, que não se resume em digitais, sendo uma análise do corpo do indivíduo, retirando dados muitas vezes alheios ao próprio titular. Esta análise de dados pode ser tão complexa que inclusive dados neurológicos são adicionados à equação, diferenciando indivíduo por indivíduo baseado no ambiente onde se encontra, entre outros diferenciais base como idade e gênero, um exemplo do que esse tipo de informação pode fazer é a forma como revolucionou a publicidade no mundo, expandindo o conhecimento sobre o público alvo.

É fato que dentre as criações da humanidade, a que evoluiu mais rapidamente foi a tecnologia moderna, gerando abismais mudanças sociais, econômicas e culturais, revoluções estas, que até hoje ainda não conseguimos quantificar precisamente. A *internet*, que surgiu em 1960, com o passar de cada ano, estima-se, que cresce aproximadamente quatro vezes a velocidade da economia mundial, em relação à sua quantidade de dados, que hoje se encontra com o percentual de 98% do total de informações que o mundo gerou, restando apenas 2% desse total que se encontra em mídia analógica.

Schönberger e Cukier (2013. p. 6) fizeram uma comparação entre marcos de invenções da humanidade e analisaram suas consequências e motivos, concluindo que:

Os aquedutos permitiram o crescimento das cidades; a imprensa facilitou o Iluminismo, e os jornais permitiram a ascensão do Estado. Mas essas infraestruturas estavam voltadas para o fluxo –de água e de conhecimento, assim como o telefone e a internet. Em contrapartida, a dataficação representa um essencial enriquecimento da compreensão humana. Com a ajuda do Big Data, não mais veremos o mundo” como uma sequência de acontecimentos explicados como fenômenos naturais ou sociais, e sim como um Universo composto essencialmente por informações.

Ao analisar o descrito, notamos que o simples fato da existência desta ferramenta de armazenamento de dados em massa, a sociedade como um todo se torna o centro da evolução, possuindo toda essa informação e transformando as dimensões de percepção à sua volta em dados que poderão ser posteriormente analisados e quantificados para inúmeros tipos de finalidades.

Não há qualquer espaço para dúvida a respeito da utilidade dos dados pessoais para a sociedade, com base neles somos permitidos de produzir inimagináveis quantidades de informação, de pesquisas científicas que analisam dados biológicos, médicos e comportamentais em busca de soluções para doenças que afetam a humanidade até à projetos que *marketing* que visem o aumento significativo das vendas de um negócio por utilizar de redes de dados que possuam informações relevantes sobre o perfil do público.

Entretanto, existem duas polaridades, a toda essa evolução que nos trouxe pontos positivos e negativos, à medida que caminhamos para soluções mais práticas e simples para os maiores de nossos problemas, também é possível agregar práticas negativas. Ao tempo que autores discorrem sobre a possibilidade de no futuro toda e qualquer informação inerente à cada indivíduo seja de amplo conhecimento público, outros dizem que é de vital importância não deixar isso ocorrer. Os estudos sobre o passado, o presente e o futuro de como nossos dados são tratados ainda é muito novo, assim como a *internet*, porém, diferente dela, caminhamos em um passo infinitamente mais lento de compreensão e análise do que o avanço diário das tecnologias ao nosso redor.

## 1.2 DO MARCO CIVIL DA INTERNET

A Lei nº 12.965, de 23 de abril de 2014, popularmente conhecida como o Marco Civil da *Internet* veio para auxiliar uma sociedade que se baseia amplamente em informação, e por meio desse auxílio procurar reafirmar que a liberdade de expressão, a neutralidade de rede e a proteção da privacidade dos usuários, constituindo assim, ponto vital na garantia da privacidade de dados do indivíduo.

Este pode ser considerado o primeiro avanço significativo sobre o tema da proteção de dados no Brasil. Trouxe maior clareza à questão, formulando texto legal sobre a proteção de dados pessoais, tendo como base leis vigentes em outros países e funcionando, em muitos casos, como uma Lei específica do assunto. Pode ser compreendido como um esforço positivo para

a regulamentação da *internet*, posto que, anteriormente, ressalta Azevedo (2014, p. 80):

O acesso aos dados e o registro da conduta de seus usuários eram plenamente destituídos de regulação específica, o que também permitiu que a internet se tornasse um ambiente hostil e de cometimento de abusos e violações de direitos. Um exemplo disso está na coleta deliberada de dados sigilosos, tanto em relação às informações quanto ao histórico de navegação em sites da internet, bem como a frequente solicitação de tempo e conteúdo por autoridades públicas sem submissão à prévia análise judicial.

A proteção de dados pessoais na internet foi um dos assuntos principais do Marco Civil da *Internet*, considerando que sua formulação foi também uma resposta ao Projeto de Lei nº 84/1999, popularmente conhecido como “Lei Azeredo”, devido a isso, deve-se analisar alguns artigos fundamentais para entender a necessidade de uma lei específica, além de ser possível por meio desse estudo compreender o significado de alguns termos importantes para a regulamentação dos dados pessoais.

O Marco Civil da *Internet* estabeleceu como princípio a privacidade e a proteção de dados pessoais, como já explanado, mas alguns pontos foram fortemente criticados, apesar da tentativa de detalhar o tema de proteção de dados.

Dessa forma, uma Lei específica é imprescindível para que haja uma mensagem clara tanto para as empresas e o próprio governo, como principalmente para o cidadão leigo compreender o funcionamento do espaço virtual.

Razão para tudo isso, como nota-se amplamente hoje, é que o direito à privacidade é de vasta importância, uma realidade farta de questões políticas e ordenamentos de questão social. Mais importante ainda é o reconhecimento de que as relações pessoais mudaram com o enorme uso da *internet* e sua infinita capacidade de processar, armazenar, compilar, compartilhar e analisar dados, com alta velocidade e baixo custo.

Não se tratando somente do setor econômico, a lei do Marco Civil da *Internet* também se preocupa com a guarda estatal, buscando regular o tratamento de bases de dados que podem extrair informações importantes e tipificar crimes antes fora do alcance da lei, por seu contexto.

Outro fator que acalorou discussões dentro do texto do Marco Civil da *Internet*, se trata da “neutralidade de rede”, conceito este que é devido ao professor Tim Wu (2010) que em foi o primeiro a trazer para o seu ordenamento jurídico pátrio no Chile. Neutralidade de rede consiste em proibir provedores e prestadores de bloquearem ou reduzirem a velocidade de tráfego de informações, preservando a integridade e segurança da rede.

No ordenamento jurídico brasileiro, a neutralidade de rede no texto do Marco Civil da Internet tipifica em seu 9º artigo, o princípio em solo brasileiro:

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

Percebe-se então que se trata de um princípio no qual o tráfego da *internet* deve ser tratado igualmente, sem discriminação, restrição ou interferência independente do emissor, recipiente, tipo ou conteúdo, de forma que a liberdade dos usuários de internet não seja restringida pelo favorecimento ou desfavorecimento de transmissões do tráfego da *internet* associado a conteúdos, serviços, aplicações ou dispositivos particulares. Em resumo, uma operadora não pode controlar o tráfego de internet de uma pessoa, tornando o acesso ruim enquanto opera, por exemplo, o *WhatsApp*, em favor do *Skype*, que teria um acesso melhor, devido ao controle da operadora.

### 1.3 DOS DADOS PESSOAIS

A definição de Mendes (2014. p. 171.), conceitua Dados Pessoais como "informação em potencial, isto é, tudo pode se transformar em informação se for comunicado, recebido e compreendido" sendo estas informações passíveis de serem codificadas e formatadas por diferentes meios e modelos.

Segundo Doneda (2006. p. 1), é vital esclarecer o diferencial entre "dados" e "informações", com foco em evitar confusões, sendo que se

diferenciam substancialmente. Assim sendo, dados são aqueles que se encontram em estado de pré-análise, antes mesmo de qualquer sistema ou indivíduo os detalhar, sendo o estado "bruto" da informação, a informação, por outro lado, se entende por ser o tratamento e a interpretação que são conferidos aos referidos dados, extraindo conhecimento, podendo agregar em seu conteúdo fatos alheios ao fato da análise. Com isto em mente, nota-se que o fator que gera tamanha eficiência e amplitude na coleta de informações é exatamente o tecnológico, transformando constantemente informações em dados, que podem ser mais bem distinguidos e organizados, para uma melhor análise.

Antes, apenas com a Lei do Marco Civil da *Internet*, não se tinha dado definição ao que seria, aos olhos da lei, dados pessoais, porém, atualmente, com a aprovação da LGPD, o conceito de dados pessoais finalmente se vê definido em regulamentação específica, sendo positivado clara e uniformemente no art. 5º, I, da LGPD, “para os fins desta Lei, considera-se dado pessoal: informação relacionada a pessoa natural identificada ou identificável.”.

Tendo em mente que a internet no Brasil começou a ser operada nos anos 90, nota-se uma real demora do legislativo brasileiro em relação à adoção de regulamentação específica. Antes da LGPD, o Marco Civil da *Internet* brasileira, Lei nº 12.527/2011, em seu 5º artigo, faz classificação de termos que seriam de grande importância, porém, apesar de em seu texto fazer várias referências aos "dados pessoais" não se encontra nenhuma definição específica e clara de seu conceito definido, trazendo consigo apenas o termo "informação pessoal", como se vê em seu Art 4º, IV, “Para os efeitos desta Lei, considera-se: informação pessoal: aquela relacionada à pessoa natural identificada ou identificável.”.

Em relatório direcionado à Câmara dos Deputados em específico a Comissão especial que lidava com a proteção e o tratamento dos dados pessoais, o IDEC (Instituto Brasileiro de Defesa do Consumidor), propõe, juntamente de empresas, que a definição de dados pessoais seja apenas aqueles que identifiquem de forma precisa o titular, texto que almejava mudar o entendimento da redação que define os dados pessoais para restrito, em razão

de que em sua amplitude tornaria praticamente qualquer atividade humana em relação à dados sujeita à lei.

O IDEC defende que o vocabulário “identificável”, da lei, seria a “mina de ouro” dos dados coletados, pois, com a sua combinação com outro dado seria possível gerar perfis completos de indivíduos, abrindo espaço para uso extensivo contra o titular. A legislação brasileira, até o momento, pouco fez em relação à isso, mantendo referido vocabulário inclusive na nova LGPD.

### 1.3.1 DOS DADOS SENSÍVEIS

Categorizados como dados pessoais sensíveis, inicialmente, são aqueles que de forma precisa relacionam indivíduos utilizando dados referentes à religião, sexualidade e até informação genética, sendo estes relacionados à intimidade da pessoa.

A CF/1988, no texto do art. 5º traz de forma expressa o que poderiam ser dados sensíveis, e um possível rol. Entretanto, esta forma de dados urge por maior amparo, uma vez que identificar estes dados pode ser problemático, isto se dá pela maleabilidade inerente à toda essa informação, relacionados ao momento e à finalidade de cada análise, tornando difícil definir quais dados seriam estes. Na pesquisa realizada por Rodrigues (2017, p.15), conclui-se que:

(...) juristas vêm se apresentando relutantes em definirem um conjunto de informações que possam ser declaradas, per se, sensíveis, sem considerar todo o contexto de sua utilização, publicização ou outras formas de tratamento. Nesta mesma linha, podemos verificar a Declaração Internacional sobre Dados Genéticos Humanos da Unesco (DIDGH), salientando que tais dados serão especialmente protegidos em função de seu contexto (HAMMERSCHMIDT, 2008). Em contrapartida, no entanto, a maioria dos Estados membros da União Europeia já apresentam um arraigado pensamento de que existiriam certas categorias de dados que sempre seriam capazes de lesar a esfera íntima da pessoa.

Mais uma vez, é hora de lei específica trazer esta definição para que se possa trazer o devido amparo, necessidade esta que finalmente é atendida pela LGPD (Lei nº 13.709/2018), onde traz em seu art. 5º inciso II:

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

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;

Este texto está diretamente adequado à 46ª Diretriz Europeia de 1995, onde proíbe que sem o consentimento do titular, o uso de dados referentes à “origem racial ou étnica, opiniões políticas, crenças religiosas e filosóficas, filiação sindical, bem como tratamento de dados relativos à saúde e à vida sexual”. Referida Diretriz foi revogada, entretanto, seus valores foram reafirmados no Regulamento da União Europeia 2016/679:

Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas.

No regulamento europeu nota-se claras intenções almejando uma classificação independente de contexto, fato é que estes dados são passíveis de abusos de privacidade e assim merecem maior proteção, tornando válido aos titulares disporem de ampla proteção jurídica, norteamo este, que ainda não se viu no ordenamento brasileiro.

### 1.3.2 DOS DADOS ANÔNIMOS

Em outra direção, existem os dados anônimos, também recentemente abordado pela nova LGPD em seu artigo 5º, inciso III:

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

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Acontece, que com a tecnologia envolvida atualmente e amplitude da captação de dados a chance de existirem dados completamente inidentificáveis é extremamente rara, vista que a forma como o cruzamento de dados é feita.

Por este motivo, o ordenamento traz outra forma de proteção à intimidade do indivíduo, a anonimização dos dados, prática esta que se refere ao tratamento aplicado aos dados sensíveis, utilizando-se da randomização e pseudo anonimização. Esta prática consiste em tentar limitar dados que identifiquem o indivíduo, utilizando-se de supressão parcial de nomes, idades e até de números do CPF, tudo em nome do anonimato do dado, como se vê no art. 5º, inciso XI da LGPD:

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Tal prática gerou diversas dúvidas sobre sua legalidade, pois, como consta da CF/1988, em seu 5º artigo, o anonimato é vedado. Porém, também na CF/1988, no seu art. 220, é claro que não haverá restrição à liberdade de expressão, logo, o anonimato dos dados é positivado, em vista da intenção de proteger a vida privada, honra e imagem do indivíduo uma vez que se é compreendido que a reclusão do cidadão à vida privada é uma necessidade de todos, sendo uma vida sem privacidade uma vida sem condições para o crescimento individual de sua personalidade.

Mesmo com o uso das técnicas de anonimização, o estudo de Sweeney (2000), titulado “*simple demographics often identify people uniquely*”, mostra que o simples cruzamento de dados referentes ao CEP e ao gênero torna as pessoas únicas e identificáveis, mostrando a fragilidade da suposta anonimização.

Apesar da anonimização ser uma ferramenta que ainda precisa melhorar para oferecer maior guarda ao indivíduo, a LGPD, delibera em seu texto, que em todos os casos possíveis devem ser utilizados dados anônimos no lugar dos dados sensíveis.

## **SEÇÃO 2**

### **DA LEGISLAÇÃO BRASILEIRA**

#### **2.1 DA INSTAURAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA - LGPD**

A Lei de Proteção de Dados Pessoais (LGPD) aprovada pelo Senado, em 2018, deverá entrar em vigor após sanção ou veto do restante do projeto de lei de conversão, nos exatos termos do § 12 do art. 62 da Constituição Federal. A LGPD é composta por um conjunto de normas com intuito de dar mais segurança aos usuários de serviços digitais brasileiros. Além disso, ela muda de maneira profunda a forma como estas práticas estão estruturadas.

Válida para empresas e instituições públicas, a lei tem abrangência em todo o território nacional. Quem não se manter alinhado com as normas pode arcar com multas, advertências, publicação da infração, bloqueio de dados e outras sanções que serão de exclusividade da Autoridade Nacional de Proteção de Dados impor, na área administrativa.

A Lei de Proteção de Dados Pessoais estabelece uma série de regras para o tratamento de informações privadas, sendo aplicáveis tanto para quem utiliza de dados internamente ou compartilha registros de terceiros com parceiros estratégicos. Esta lei permite que o cidadão tenha direito de saber se a empresa possui algum dado sobre ele. Além disso o cidadão pode exigir que, caso a empresa tenha os tais dados, que eles sejam apagados

Em outras palavras, a LGPD funciona de maneira semelhante ao *General Data Protection Regulation* (GDPR) da União Europeia. Ele dá mais controle aos cidadãos sobre como as suas informações são usadas e, assim, permite a criação de um ambiente digital mais seguro e privado. De acordo com o especialista em direito cibernético, Quintiliano (2019), a diferença entre a LGPD e a GDPR, é o nível de detalhamento: “a nossa lei cobre todos os aspectos que a GDPR cobre, mas de uma forma menos detalhada. Talvez algumas questões tenham que ser disciplinadas posteriormente, mas em termos de abrangência eu entendo que são equivalentes” afirmou em entrevista dada ao Estadão.

Como demonstrado no subcapítulo anterior, a Lei nº 12.965/2014 proporcionou os primeiros passos para a redação de Lei específica sobre a proteção de dados pessoais. Além disso, houve três iniciativas legislativas que buscaram regular de forma objetiva os dados pessoais o PL nº 4.060/2012, PLS nº 330/2013 e o PL nº 5.276/2016.

O Projeto de Lei nº 5.276/2016 é o que antecede a LGPD, seguindo padrão internacional mais sólido, sendo fortemente influenciado por marcos regulatórios de países pioneiros na proteção de dados. O anteprojeto de lei do Poder Executivo também foi objeto de amplos debates públicos, “recebendo mais de 50 mil visitas e obtendo mais de 1.100 contribuições”, segundo verificação do próprio Poder. Isso demonstra a preocupação em fazer com que diversas áreas da sociedade pudessem participar de sua redação, proporcionando assim um texto com caráter democrático e coeso com a realidade, fator muito importante, uma vez que específica legislação deve passar a ser conhecida cada vez mais pela sociedade de forma diária. Apesar da votação do projeto ter sido fixada em regime de tramitação com urgência constitucional, o trâmite ocorreu durante anos até que o PL acabou não sendo aprovado e novo projeto (LGPD) tomou forma.

Formular uma lei específica é necessária não apenas para preencher as lacunas deixadas pelo Marco Civil da *Internet* e proteger melhor o cidadão, mas também deve ter a intenção de uniformizar o significado dos conceitos essenciais para a proteção de dados e coordenar as políticas internas e externas do Brasil. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) que, por meio de 65 artigos, distribuídos em dez capítulos,

aborda regras já implementadas na União Europeia, através da GDPR (2016) entre elas estão definições importantes de tratamento dos dados pessoais, os fundamentos que serão respeitados, e busca garantir a proteção dos direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

## 2.2 DA LEI GERAL DE PROTEÇÃO DE DADOS

Seguindo o exemplo do GDPR, regulamento europeu, a LGPD irá transformar o atual sistema de operações, alterando como se armazena, coleta, trata e compartilha os dados, colocando um, à muito necessário, padrão de proteção e instaura punições para quem não se adequar à norma.

Com a lei, chegam conceitos definidos de termos importantes para a esfera em questão, Entende-se por “dados pessoais” toda e qualquer informação que possa estar relacionado à alguma pessoa identificada ou que possa ser identificada através dos dados, “tratamento de dados” é o processo realizado com estes dados, englobando, como são classificados, acessados, utilizados, reproduzidos, organizados, processados, armazenados, deletados e muitos outros.

Ao se coletar e processar dados é agora dever se manter atento ao que impõe a lei, o texto da lei faz menção à nove situações que agora se serão ilícitas, com ênfase nas duas mais ocorrentes, sendo elas, a forma como se obtém o consentimento do titular e que de fato haja legítimo interesse. No caso do consentimento, se torna necessário obter o consentimento de forma explícita e clara, deixando opção de fornecer o dado ou não, a escolha deve ser livre. Ao tratar do legítimo interesse, o controlador, deverá tratar os dados de forma legítima e possuir finalidade concreta a partir do contexto da relação em questão.

Importante estar ciente também dos conceitos detalhados dos quatro principais agentes que deverão interagir de forma direta e indireta com os dados, sendo eles, o titular que nada mais é que a pessoa física ou jurídica a

quem os dados são oriundos; o controlador seria a pessoa física ou jurídica que realiza a coleta destes, determinando como será feita e para qual será sua finalidade; o operador, pessoa física ou jurídica que tratará e processará os dados seguindo orientação do controlador; o encarregado é o agente, neste caso somente pessoa física, que manterá comunicação entre o controlador, o titular e a Autoridade Nacional de Proteção de Dados, o encarregado será escolhido pelo controlador e deverá, também, instruir funcionários que o controlador possa vir a contratar.

Grande mudanças vieram com a nova lei, e com isso, grandes oportunidades positivas, empresas deverão implementar novas formas de se relacionar com seus clientes, mantendo o ambiente livre de práticas obscuras e invasivas, adquirindo uma relação mais natural e de confiança enquanto bons profissionais perceberão que se trata de um momento ótimo para apresentar táticas mais limpas e eficientes, evoluindo um mercado, pode-se nascer um sentimento de satisfação por parte do titular do dado, ao saber que está sendo bem tratado e que possui total transparência para saber o que é feito com toda sua informação, isto aufere valor à imagem da empresa e poderá inclusive reduzir o desconforto do titular ao tratar com profissionais da área.

Outra área que verá grandes benefícios será a publicidade informativa, que informa ao mesmo tempo que promove um determinado serviço ou produto, este tipo de publicidade deverá ganhar mais e mais importância com a publicação de conteúdo original por parte do encarregado e que terá real relevância ao titular. Esta técnica promoverá ainda mais o engajamento, abrindo cada vez mais espaço para uma relação ativa e natural entre todos os agentes, mantendo clara e consciente as atribuições de cada parte, ao contrário de um titular que serviria apenas para se acumular dados aleatórios, transformando assim uma relação passiva em ativa e criando um sentimento de compromisso toda vez que se adquirir a permissão de um titular.

Oportunidades vistas por meio de campanhas publicitárias deverão observar pontos importantes com a LGPD. Para que se efetive a coleta de dados de forma legítima é de vital importância que o consentimento do titular seja explícito e direto, seja uma opção do titular adentrar ou não tal situação. Esclarece a lei, que será nula toda e qualquer coleta que se dê através de opções já marcadas pelo site e que ficariam fora do campo de visão da

concedente. Na prática, é interessante que esta coleta seja feita através da realização de uma chamada, onde seriam explicitas toda a transparência da ação, que o titular poderá optar por adentrar ou não, outra opção que provavelmente se tornará mais comum, será através dos campos de *checkbox* que trarão de forma específica cada conteúdo ofertado.

Pilar fundamental de toda a estrutura que a lei traz é o vínculo dos dados (funcionando quase como um tributo vinculado), deverão agora, ser utilizados somente para com suas finalidades, que deverão ser predeterminadas e explícitas no momento da concessão pelo titular, limitando que seja requisitado apenas o necessário para finalidade específica do momento. Outra prática que também se torna ilegal é a de organizações e empresas que utilizam de terceiros para comprar listas prontas contendo dados de titulares e entrar em contato desta forma, esta prática, mais comumente vista com listas de e-mails ou telefones não se dará mais por ir contra princípios cruciais da lei, ferindo a transparência e a finalidade para qual esses dados foram adquiridos.

O foco deste é tornar todos os dados adquiridos em dados adquiridos com permissão direta, exigindo também permissão inclusive para contatar o titular. Neste caso, deverão analisar todos os bancos de dados que já possuem, e assim, identificar quais seriam válidos, documentando e especificando quais seriam com ou sem consentimento e quais vieram de terceiros. Esta documentação é de grande importância, visto que a nova lei conta com a boa-fé e diligência de todos.

O *marketing* que se utiliza de dados comportamentais e informações sobre um grupo-alvo específico se tornará um real desafio em razão da ciência de cada titular em conceder tais informações para que sejam utilizadas com esta finalidade. Até a vigência da GDPR, o *Facebook*, utilizava do pretexto de coletar informações para proporcionar ao usuário uma “melhor experiência”, argumento que se provou falso diversas vezes, advindas de todos os escândalos de privacidade e processos legais em andamento contra a rede social. Consequência disso é que possivelmente todos que criaram uma conta na referida rede, agora tem seus dados convertidos em gráficos e perfis específicos, dependendo do contexto no qual são inseridos, documentando do

comportamento de cada um na rede, até acessos em sites vinculados com o mesmo.

Sites que lidam com dados deverão agora tornar de fácil acesso e de maneira clara a possibilidade de que os titulares possam a qualquer momento acessar e se informar sobre quais dados estão sendo utilizados pelas empresa, além de exigir que aja sido conquistada a permissão de quem origina o dado, podendo também recusar que algum dado seja tramitado. Ponto importante a se notar é toda a particularidade que envolve a rede social mais famosa da nossa internet, o *Facebook*, que passará a acarretar uma enorme responsabilidade e diversas obrigações sendo que poderá englobar o papel de dois agentes específicos, o de controlador e o de operador. Entretanto, a empresa à tempos já busca se adequar à GDPR e assim, quem fica mais exposto seria exatamente a empresa de menor porte que busca realizar campanha na rede social, assumindo papel de controlador neste caso, contraindo responsabilidades de organização e assim devendo utilizar-se de meios que mantenham a transparência.

Técnica amplamente utilizada no mercado atual é o remarketing, esta consiste no direcionamento da informação, isso significa que através da compreensão de determinado perfil de comprador a empresa pode adaptar sua proposta para que ela se adeque especificadamente à alguma classe. O indivíduo, ao adentrar determinado site, seja para ver um vídeo ou ler um artigo, poderá, a partir da técnica de remarketing, entrar em contato com um anúncio totalmente personalizado para sua experiência individual, isso significa que outro indivíduo com outros interesses e personalidade também receberá um anúncio diferente e ao mesmo tempo, salvando no banco de dados de referido site os denominados *cookies* (dados salvos resultantes de uma interação particular na internet) e os enviando direta à algum banco de dados que no futuro, com base no que foi lido e interagido no site supracitado, poderá vir a personalizar ainda mais as futuras experiências do titular. Referida metodologia deverá passar por medidas mais rigorosas, onde o controlador deverá passar a informar o titular que está salvando sua atividade no site e a sua finalidade.

Importante notar no texto da lei que em casos em que o titular dos direitos sofra quaisquer danos em razão de seus dados, o controlador e o

operador responderão solidariamente, responsabilidade igualmente dividida entre as partes. Entretanto, caso que merece maior atenção seria nas ocasiões em que alguma organização esteja ocupando o lugar de agente controlador de uma operação, isto é, sendo ela que tomará decisões sobre procedimento e finalidade o operador do caso poderá conseguir se livrar de responsabilização, provando, claro, que não seja passivo de culpa, restando essa à ação de terceiros ou erro por parte do titular.

Pode parecer assustador mudanças tão radicais nos costumes já fixados na forma de como essas operações são tratadas, entretanto é uma mudança de extrema importância e que deverá acontecer mais cedo ou mais tarde e quanto mais cedo, maiores problemas serão evitados no futuro. A legislação dificulta diversos pontos, mas também traz incrível oportunidades de se aprimorar e construir uma relação mais efetiva e real entre as partes, mas é fato que essas oportunidades deverão representar muito mais do que uma simples notificação informando que a política de privacidade, foi atualizada.

### 2.3 – DOS PRINCÍPIOS DOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados no seu 6º artigo, traz um muito aguardado e necessário rol de princípios a serem seguidos no tratamento dos dados, sendo eles previstos na lei em sua totalidade por 10, são eles:

O Princípio da finalidade diz ser necessário explicitar a finalidade que o controlador dará aos dados, sendo ela específica e informada ao titular, sendo a prática totalmente incomum até a vigência da lei. Exemplo atual seriam todos os dados que consentimos em fornecer ao *Facebook*, imagine que anos atrás, ao criar uma conta na referida rede social se pensava que suas informações estariam sendo utilizadas para serem compartilhadas com amigos e hoje, anos após, com toda a proporção que a rede social tomou e suas inúmeras ramificações, estes mesmo dados continuam a ser processados e não podemos começar a imaginar para quais finalidades estão sendo utilizados, e desta forma se torna ilegal o uso destes dados pelas empresas ou organizações que os recebem e fazem o que querem destes dados.

O princípio da adequação trata que se deve manter um comportamento compatível com o que foi previamente informado ao titular, assim como manter uma relação coesa com o contexto do dado tratado. Como exemplo neste caso, pode-se referir à compra de um sapato qualquer no ambiente virtual, onde para finalizar a compra o site solicita informações a respeito de seu grau de instrução escolar, caso este, estaria incompatível com o contexto aparente, portanto se torna ilegal.

O princípio da necessidade, este princípio instrui que a partir da vigência da lei, existirá um grau de responsabilidade, sendo essa crescente proporcionalmente à quantidade de dados que uma empresa teria acesso, assim como limitar os dados utilizados, determinando assim a que sejam utilizados apenas os dados necessários para aquele contexto, deixando de se agregar dados abrangentes que possam a ser convenientes para outros assuntos.

O princípio do livre acesso seria a garantia de que todo titular do dado, pode checar facilmente e gratuitamente a forma como são tratados os dados e por quanto tempo eles estarão disponíveis ao controlador, princípio este que permite uma fiscalização direta do titular.

Princípio da qualidade dos dados, este, torna necessária a clareza e a atualização por parte de quem solicita os dados, a respeito da sua finalidade, mantendo sempre o titular ciente da forma mais objetiva possível e atualizado, caso haja alguma mudança no tratamento.

O princípio da transparência traz que todas informações declarada devem ser, em todos meios de comunicação, claras, verdadeiras e de fácil acesso, mesmo que observados segredos comerciais da empresa, se torna ilegal o repasse a terceiros sem que haja anúncio ao titular.

O princípio da segurança, instaura que será de responsabilidade da organização ou empresa o controle por meios administrativos e técnicos de proteção aos dados, sendo isto em foco na prevenção de invasões de hackers, perda, destruição, difusão, alteração, ou quaisquer outros modos que possa causar dano ao titular.

O princípio da prevenção traz algo que se mostrará de grande eficácia caso de fato praticado, pois impõe a necessidade de medidas preventivas no que tangente do que pode se tornar um problema, ao contrário

de lidar com os problemas depois que aparecem, evitando o dano em primeira instância.

O princípio da não-discriminação é sem dúvida, um dos mais importantes princípios que recebemos com a nova lei, ele traz um controle à muito necessário ao controle dos dados. Em sua redação, traz que não deverão ser utilizados os dados de forma à discriminar ou promover quaisquer tipos de abusos aos titulares, um exemplo claro, se trataria de uma empresa imobiliária onde com os dados que auferiu de seus clientes, seja por meios próprios ou de terceiros, utiliza destes dados para traçar perfis, conseguindo, extrair o comportamento destes titulares, assim determinando talvez uma melhor capacidade de pagar, uma probabilidade maior de vender à determinado perfil, e assim criar diferentes ofertas para cada perfil com base nos dados coletados. Tal prática utiliza amplamente dos dados determinados “sensíveis”, trazendo inúmeras aplicabilidades na sociedade uma vez que podem ser criados perfis econômicos, raciais, políticos, religiosos, filosóficos, genéticos, um para cada contexto existente, o que traz uma infinidade de possibilidades.

O último, mas não menos importante, o princípio da responsabilização e prestação de contas, este impõe a todos que passem pelas medidas de adequação à LGPD, devem também coletar evidências de sua concordância com as normas, em nome da boa-fé e diligência.

## 2.4 – DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Após sua criação em 27 de dezembro de 2018 através da MP nº 869, a ANPD foi vetada em seu texto original onde foi alegado haver vício de origem, pois se tratava de um órgão vinculado ao poder Legislativo, que não poderia tratar da organização do Estado, razão disto que após de alteração no texto, sendo agora vinculada ao poder Executivo, foi sancionada e se deu a Lei nº 13.853, de 8 de julho de 2019.

É assunto delicado qual Poder deveria estar vinculado ao órgão nacional que irá gerir os pontos mais importantes na proteção dos dados

peçoais do cidadão brasileiro, incluindo agir como órgão fiscalizador, elaborador de diretrizes e aplicador de sanções administrativas. Mesmo que criada em situação de calamidade pública e difícil cenário político e meio que “às pressas” para estar de acordo com a vigência da LGPD, o controle do órgão deveria ser mais bem guardado, diferentemente de submetido à um dos Poderes, é o que disse o presidente da Câmara dos Deputados, Maia (2020):

“O ideal é que a agência não fosse vinculada ao governo. A criação da agência debaixo da estrutura do governo foi errada. Quem tiver o comando dos dados talvez tenha o comando do País por muito tempo, por isso é importante ter uma agência de proteção de dados distante do governo”

Com o supracitado comentário, o presidente da Câmara traz à frente preocupação real no que tange ao poder inerente aos dados e o que as empresas e organizações de hoje são capaz de fazer ao utiliza-los, a nova legislação vem principalmente como meio de controlar e limitar tais ações, então, nada mais lógico que manter o órgão que irá monitorar tudo isso o mais guardado possível de quaisquer interferências políticas entre os Poderes.

## **SEÇÃO 3**

### **DADOS E A PRIVACIDADE**

#### **3.1 – DO USO DOS DADOS**

No mundo moderno, com quase todos possuindo algum modelo de *smartphone*, é uma situação comum onde por vezes se pondera se o seu celular está ouvindo suas conversas, pois logo após uma conversa com algum amigo sobre determinado produto ele logo aparece em diversos anúncios em vários sites e redes sociais que frequentamos, isso se trata, na realidade, do maior experimento psicológico que a humanidade já viveu, englobando todos que tenham contas na internet e mesmo quem nunca nem entrou na plataforma. O *Facebook*, empresa que muitas vezes já citada neste trabalho, e

devidamente, será mais uma vez o foco de análise na intenção de se projetar as dimensões possíveis a serem tomadas quando se trata de dados. A empresa se tornou uma entidade que ultrapassa qualquer país do mundo, tendo mais de 2,7 bilhões de usuários até o meio de 2020, sendo 140 milhões brasileiros que acessaram diariamente em 2019, mesmo que um indivíduo não faça parte do *Facebook*, muito provavelmente ainda possuirá uma conta no *Instagram* e caso isso também não, no Brasil é garantido que o indivíduo tenha um número de *WhatsApp*, plataformas estas que entre outras, são da mesma companhia.

Detalhe importante ao compreender a rede social é conhecer do surgimento do *Facebook*, com um explosivo começo, ainda lhes restava uma coisa, como fazer dinheiro em um modelo de negócio que antes falhou tantas vezes antes. Seu maior enigma foi desvendar como atrair quem tem dinheiro para gastar na internet, que já faziam isso em outras plataformas, quem já sabia o que adquirir ia para o Google para saber onde comprar e quem já sabia o que desejava e sabia onde comprar, ia para a *Amazon*, com os maiores espaços que lidam com compra na internet já ocupados por gigantes, o *Facebook* decidiu tomar outra rota, convencer o indivíduo a comprar, criar desejo nas pessoas, este se tornou seu papel na internet, saber tanto sobre o indivíduo que ele não precise ir a nenhum outro lugar, tudo que ele precisa já está ali e antes mesmo de perceber, a rede social conheceria o indivíduo tão bem que passaria a ter o que nenhum governo nem entidade no mundo tem, acesso a como as pessoas se sentem. É de fato fascinante e assustador o quanto esta rede social pode entender a humanidade como ninguém e com o modelo de negócio que o *Facebook* opera, e a forma que gera dinheiro, isto se torna ainda mais assustador.

Um exemplo importante para se entender o método de negócios do *Facebook* é pensar em uma propaganda qualquer de cerveja, um anúncio destes em bons horários geralmente custam uma fortuna para quem adquiriu o direito de transmiti-la, mas acontece que este formato possui um desperdício gigantesco, sendo que ele é mostrado a todos, pessoas que não bebem podem até mudar de canal se for o caso, enquanto apenas alguns da parcela de público alvo seria realmente convencido pelo anúncio, por outro lado, ao analisar o sistema do *Facebook*, percebe-se que não há necessidade de

mostrar um anúncio de cerveja para quem não bebe, o importante é que eles sabem o que o titular dos dados quer e assim podem então ofertar para quem consome álcool, anúncios de cerveja e para quem não bebe, um suco ou refrigerante, mostrando o anúncio apenas para compradores em potencial, anulando o desperdício inerente ao anúncio de TV, a estratégia adotada em saber e apresentar para o indivíduo o que ele irá desejar antes mesmo que lhe passe à mente ir no *Google* procurar ou na *Amazon* comprar se mostrou de enorme eficácia, seu principal foco não é mais a felicidade do indivíduo ao engajar com a rede social, mas sim o puro engajamento, o mais tempo possível para que gere a maior quantidade de informação possível para assim compreender e prever o comportamento de cada um com mais precisão. Em suma, o modelo praticado se preocupa em atrair marcas ou empresas que utilização de suas ferramentas para vender mais produtos e não o titular dos dados que entrega a informação de graça e sem nem saber.

Tudo que é postado por um titular, tudo que é compartilhado, tudo que é curtido ou comentado é facilmente interpretado por algoritmos que, sem ao menos ver uma foto do rosto do indivíduo, com precisão podem determinar etnia, postura política, religião, se a pessoa tem depressão, se é inteligente, o relacionamento com os pais, orientação sexual, situação financeira e um infinito de outros dados que podem ser extraídos de diversos tipos de indivíduos. É bem possível que o *Facebook* saiba mais sobre uma pessoa do que ela mesma, através de algoritmos e Inteligência Artificial, como o estudo "*Computer-based personality judgments are more accurate than those made by humans*" mostra, com apenas 10 curtidas que o indivíduo dá na rede social já é o suficiente para traçar um perfil de personalidade mais preciso do que um colega de trabalho diria sobre o titular, com 70, um amigo, com 150, um familiar, com 300, se mostra mais eficiente em determinar o que a pessoa gostaria do que um cônjuge, isto mostra que a rede social possui capacidade de saber muito mais sobre alguém do que as próprias pessoas com quem convive e quanto mais atividade, mais dados e quanto mais dados, mais preciso será seu perfil virtual.

Esta análise se aprofunda tanto que passou a identificar precisamente o estado emocional das pessoas acompanhando padrões de postagem, pesquisa esta, que foram publicados inclusive pelo grupo de

cientistas de dados do *Facebook*, mostrando como identificar momentos de felicidade das pessoas através de sua atividade na rede, indicando inclusive que este seria o momento ideal para começar a oferecer produtos à este indivíduo, visto que pessoas em estado emocional feliz, tendem a comprar mais. Outro ponto disso tudo é que não precisam de curtidas para se determinar o estado emocional de um indivíduo, o estudo "*Instagram photos reveal predictive markers of depression*" mostra a capacidade de algoritmos e inteligências artificiais em dizer precisamente se uma pessoa está depressiva ou feliz apenas pelas cores predominantes em postagens no *Instagram* de alguém. O algoritmo específico citado foi mais preciso em prever quem teria um diagnóstico de depressão do que especialistas treinados da área e se apenas com as cores predominantes no contexto de um indivíduo é possível dizer tanto, diversas outras aplicabilidades são possíveis.

Nota-se, com o avanço do *Facebook*, que a rede agora está integrada em diversos outros sites, efetivando cadastros rápidos ou até compartilhando alguma informação de um blog paralelo, isso se deve aos códigos entrelaçados, estes códigos possibilitam ao *Facebook* saber sempre por onde o titular navega, onde interage, e com o quê interage, e sempre coletando dados que irão incrementar o perfil individual. Com tantas ferramentas que existem para rastrear nossa interação na internet, e seu constante desenvolvimento e refinamento, chegamos a um momento onde mesmo quem nem *Internet* tem, ele ainda poderá ser rastreado e quantificado pelos inúmeros sistemas de coleta de dados. Através de amigos, família ou até conhecidos, que possam vir a citar um indivíduo, postar fotos onde ele esteja presente, ligar para esse indivíduo ou se este indivíduo está na lista de contatos do celular que foi compartilhada com alguma rede social, qualquer uma destas já é o suficiente para que este indivíduo particular seja categorizado. Esta categorização se baseia nas preferências comuns entre o círculo de amigos ou familiar de uma determinada pessoa, se possuem muitos amigos que assistem muitos filmes, esta pessoa provavelmente também assiste muitos filmes, se tem muitos familiares que praticam esportes diariamente, provavelmente também os pratica, também utiliza como base o que seus círculos de amigos andam comprando para poder lhe oferecer uma proposta mais adequada. O *Facebook* já sabe o indivíduo quer, sabe o que lhe

oferecer, ele possui os dados do titular e os dados de pessoas que convivem com ele, e estes mesmo dados são mais informativos na hora de criar uma campanha publicitária para algum público alvo específico do que o que indivíduo pensa na sua máxima particularidade, através de uma análise comportamental generalizada é facilmente determinável muitos aspectos da vida de alguém, inclusive o melhor momento para lhe fazer ofertas.

Como dito previamente, pode-se concluir que estas redes sociais ligam o microfone dos celulares para poderem ouvir a conversa das pessoas, mas a realidade é bem diferente, elas não precisam fazer isso, tudo é coletado de forma muito mais profunda e precisa, extraíndo informações sobre conversas que ainda poderão ocorrer, não é nem mesmo necessário ter acesso direto ao titular para adentrar sua privacidade.

Este tipo de tecnologia, em especial, a desenvolvida diretamente pelo *Facebook*, é baseada na qualidade de um determinado algoritmo utilizado para quantificar certa informação, ocorre que, com uma base de usuários maior de qualquer país no mundo, que cresce a cada instante, é inteiramente viável testar livremente a eficácia destes em questão de minutos, alcançando questões que podem ser fracionadas em pequenos grupos de pessoas, até a questões extremamente complexas que necessitariam de milhões de pessoas para se alcançar uma resposta. É impossível para qualquer país ou empresa no mundo fazer o que o *Facebook* faz, a velocidade no qual esse tipo de inteligência evolui lá é espantadora e a informação tirada inclusive de formas indiretas é tão útil quanto a que o indivíduo analisado possui sobre si mesmo, tornando o *Facebook* a maior mineradora de ouro digital do ocidente, o tornando a entidade mais poderosa do nosso mundo no tangente ao que pode causar à realidade individual de cada pessoa, ele não fala através de uma televisão para tentar agradar a todos de forma homogênea que ali estão ouvindo, ele aguarda a melhor oportunidade para falar com o alguém individualmente e das formas mais sutis possíveis, este é o maior experimento psicológico em massa que vimos até os dias de hoje.

O grande problema do mundo moderno começa quando essa sistemática deixa de agir de um polo passivo (analisa informação e sugere algo baseado no contexto) e passa a agir de forma ativa (sugere sentimentos para alterar um contexto), em 2010, foi publicado um estudo pelo próprio *Facebook*

que, durante um único dia, experimentou adicionar um broche a cada postagem de um usuário que votou nas eleições presidenciais da época, tal broche, sendo visto por amigos, família, conhecidos e até por uma simples concordância social de ver o próximo realizar o ato, aumentou consideravelmente o número de pessoas que se dirigiram a votar, tendo em vista que lá o voto é opcional. Esta ação em si, ainda é considerado ato bem neutro, uma vez que o voto é opcional e não direcionava a qualquer tendência, mas e se este pequeno incentivo se tornar mais agressivo, e se ele incluir um grupo político e outro não, e se for apresentado apenas para uma etnia, e se ele excluir uma religião, isto seria o suficiente para decidir uma eleição.

No ano de 2014, o *Facebook* publicou a pesquisa “*Experimental evidence of massive-scale emotional contagion through social networks*”, desta vez, testaram as emoções das pessoas, 689,003 mil usuários, sem que soubessem, foram alvos de postagens de cunho à gerar sentimentos negativos ou positivos e foi o que aconteceu, o resultado confirmou que de fato as pessoas foram contaminadas com as emoções provocadas, o efeito relatado foi de baixa escala, entretanto, estava lá. Não seria adversidade pensar que rotular esse tipo de experimento como sinistro, antiético e de gigantesca intromissão na vida particular dos experimentados, considerando ainda que o controle total do que aparece ou não para um indivíduo é inteiramente de decisão da empresa, tudo possível quando o usuário passa por aquelas muralhas de textos ao criar uma conta, que na realidade, até então não seria nem possível julgar alguém por não perceber as consequências, uma vez que nem descritas ali estavam.

Após referidos estudos publicados, a empresa sofreu enorme repercussão negativa, instaurados processos que continuam em tramite a anos e com isso, pararam de publicar quaisquer estudos desde então, isso não significa que não realizam mais estes experimentos e não significa que o *Facebook* perdeu clientela. Uma plataforma que ao utilizar das informações de todos seus usuários têm acesso a como bilhões de pessoas pensam e se comportam e assim capaz de criar propagandas eficientes e baratas e aprimorá-las em uma velocidade espantosa, acaba por atrair todo tipo de anunciante e todo tipo de indivíduo e empresa que deseja saber ou mudar, como tanta gente pensa. No ano de 2018, ocorreu o maior escândalo datado

envolvendo o *Facebook*, sendo revelado que nas eleições de 2016 a *Cambridge Analytica*, teria coletado dados de usuários com o auxílio do *Facebook* para vendê-los à campanha política de um dos partidos concorrentes das eleições na época, este tipo de escândalo, pode chocar todos os usuários quando ficam sabendo, mas para quem tem intenções de utilizar das ferramentas da plataforma, não se poderia ter um “anúncio publicitário” tão efetivo quanto este, visto que se a rede social consegue alterar o curso de uma eleição presidencial, ela confiantemente poderá vender o produto de seus clientes.

É notável que apesar do tamanho do *Facebook*, mais e mais pessoas deixam de utilizar a rede social como a sua principal, mas em compensação o *Instagram* cresce em velocidade proporcional e o *WhatsApp* também, como visto principalmente no Brasil, e por serem todos da mesma organização, no final das contas não perdem muitos usuários, inclusive, com a pandemia que afeta nossa sociedade, as ações do *Facebook* cresceram bastante com grande parte da população em casa.

Nem todos os casos citados nessa seção são intrinsecamente bons ou ruins para a sociedade, o avanço da tecnologia tem sempre o potencial para ser usado de maneira positiva, provendo ótima comodidade, espalhando ideias positivas e compartilhando conhecimento, assim como de maneira negativa, invadindo a privacidade do indivíduo, controlando formas de pensar e automatizando interações sociais. Como previamente dito, o principal problema aqui é para tudo que aqui foi descrito, seja bom ou seja ruim, envolve abrir mão da privacidade e cada vez mais abrir mão da autonomia, permitindo que nossas próprias emoções sejam quantificadas e alteradas pelas redes sociais sem qualquer conhecimento do usuário desprotegido que ali navega diariamente. Por todos estes casos que devemos conhecer e nos informar para que possamos utilizar ao máximo as capacidades que as novas legislações de proteção aos dados que se instauram no Brasil e por todo o mundo da melhor forma possível onde podemos procurar construir uma relação saudável entre todas as partes, ao contrário de gerar sentimentos negativos nas pessoas essa tecnologia tem a capacidade de incentivar a população a se educar, se vacinar, ajudar o próximo, usar máscara, entre infinitas outras e quanto mais evoluída é

a tecnologia, mais potencial ela carrega e até agora é evidente que não se utiliza muito do seu bom aspecto.

### 3.2 DA PRIVACIDADE

A privacidade pode ser o conceito mais importante do nosso tempo, ela permite definir todo o contexto a nossa volta, sem ela é impossível saber quais normas regem, as vidas da população serão julgadas baseadas em regras e caprichos das organizações que as gerem.

Inúmeros já perderam seus empregos, outros perderam todos seus círculos de amigos, outros perderam até a vida, coisas que ditas na suposta privacidade que deveria ser direito de todos, por vezes, acabam vazando para o público geral e isto, pode ter consequências preocupantes. Nesse tipo de situação, o público ao analisar uma situação específica pode julgar uma pessoa mediante suas ações expostas, entretanto, estas ações podem não estar alinhadas com a intenção real do indivíduo, ou mesmo seu contexto, levando à possível ruína de uma pessoa.

Ao primeiro olhar é possível entender que existe sim um lado bom para isso, afinal, ações negativas devem ser tratadas de adequada maneira, entretanto, o assunto é mais complicado do que isso. A liberdade de expressão é um direito relacionado à esfera pública, sempre foi possível dizer o que bem entender na particularidade do indivíduo pelo simples fato de que não era possível haver qualquer interferência externa, e no caso de que agora o privado se tornou público, é necessário evitar que a liberdade de expressão se torne algo homogêneo e controlado por alguns ou uma completa anarquia de pensamentos.

É necessário que seja repensada a maneira de proteger a privacidade do indivíduo, os meios tradicionais não são mais efetivos, é necessária uma reavaliação dos direitos que envolvem a privacidade. Não são mais os tempos onde uma pessoa famosa fala algo em privado que possa haver controvérsias e após uma denúncia à um jornal, por exemplo, o jornalista iria investigar o caso para determinar se é verdade ou não, os tempos atuais

conferem esse poder a todos, inclusive organizações, empresas e países. Importante considerar que se ocorrem casos de notícias falsas publicadas inclusive por profissionais da área a capacidade de dano a outrem gerada por uma população inteira de internautas constantemente monitorando a vida de alguém, é muito maior.

Assim como ocorre em organizações que lidam com dados, não há julgamento das ações de um indivíduo, há o julgamento da ação filtrado pelas intenções de quem julga. Muitas vezes esse tipo de situação, quando ocorre por parte da população em reação a algo negativo de uma parte, nos tempos atuais pode gerar até linchamentos e total erradicação da vida social ou profissional desta pessoa, mesmo com as acusações sendo verdade ou não, isto não se trata de justiça. Este tipo de situação, com a crescente queda de privacidade que o mundo sofre, gera um sentimento de coesão, tendo em mente que nunca alguém iria querer estar no lugar do acusado que teve sua privacidade violada e suas ações expostas para todo o mundo, fora de contexto ou não, não é uma situação justa.

O filósofo Bentham (1785) procurou descrever a prisão perfeita, o “Panopticon”:

Apesar de ser fisicamente impossível para que um único guarda vigie todas as celas ao mesmo tempo, o fato de que os presos são incapazes de saber quando estão sendo observados significa que são motivados a agir de forma como se estivessem sendo observados a todos os momentos.”

Conceito que, com tanta tecnologia que nos cerca e vigia constantemente, vem se mostrando preocupantemente cada vez mais próximo da realidade. Com tudo isto em mente, é de vital importância que além as novas legislações mundiais obtenham sucesso em limitar as grandes controladoras de dados, a sociedade como um todo esteja mais ciente das consequências que uma má gestão de tanta informação pode trazer para a realidade de todos.

## **CONSIDERAÇÕES FINAIS**

Ao iniciar este trabalho, existiam problemáticas evidentes relacionadas que ao final se esperava encontrar a solução, ocorre que, apesar destes problemas terem de fato sido analisados, explicados e desconstruídos, é notável que com o aumento de compreensão relacionado ao assunto, propor soluções para questões tão complexas se torna cada vez um desafio maior.

Referem aos problemas pré-determinados nesta pesquisa apesar de não descritas claras soluções para os problemas em questão, é notório que uma difusão do conhecimento a respeito do que se passa e de casos específicos citados, é possível, através da informação evitar muitos destes problemas assim como deixar o leitor mais alerta quando encontrar situações semelhantes no dia a dia.

Apesar de se tratar de um estudo relativamente datado, recentemente tomou proporções gigantescas, transformando completamente a visão anterior sobre o assunto, por este motivo, a biografia referenciada ainda é muito nova e muito ainda precisa evoluir, uma vez que a compreensão humana sobre o assunto se encontra anos atrás do que vivemos hoje e o melhor que a sociedade pode fazer com a situação é buscar analisar ainda mais o tratamento que é conferido a estes dados e oferecer o máximo de proteção a aqueles possam vir a ser lesados neste processo.

Dentre o pesquisado se nota que em tempos passados, através de uma simples portaria de prédio já se era possível descobrir várias informações sobre uma pessoa, hoje então, com tantas formas de se alcançar alguém, estas informações estão até mais fáceis de serem adquiridas, incluindo também informações muito mais sensíveis e pessoais. E estes dados, em mãos de terceiros, podem significar uma conta falsa em sites, fraudes, vazamento de informações sigilosas até a quantificação destes para que seja possível extrair uma análise comportamental do indivíduo. Fato é, cada vez mais as informações que identificam um indivíduo, com todas as suas particularidades, se tornam mais e mais expostas no ambiente virtual e é de vital importância que tenham a informação para se prevenir e a proteção legal que necessitam.

Para onde vão todos esses dados, quem os gerencia e o que é feito deles, são todas questões que deveríamos passar a considerar diariamente. Informações cruciais ou altamente pessoais, no que se diz à pessoa tanto física

quanto jurídica, pode ter consequências catastróficas, causando danos até irreparáveis à imagem, ao financeiro e até à vida pessoal de um indivíduo.

Nota-se que a informação como um todo, já é visto em todo o mundo como tão valioso quanto o ouro e com potencial infinito, uma vez que se trata de um recurso infinito e merece total amparo da lei em sua proteção, assim como uma atenção redobrada do titular ao cedê-los.

## REFERÊNCIAS

AGUIAR, Filipe Silveira; LEAL, Pedro Henrique Peixoto. *Efeito translativo nos recursos extraordinários*. Jus Navigandi, Teresina, ano 12, n. 1455, 26 jun. 2007.

ALMEIDA, Vanderlei Henrique de. *Recurso Especial e Recurso Extraordinário: concessão do efeito suspensivo. Possibilidade*. Jus Navigandi, Teresina, ano 5, n. 41, 1 maio 2000. Disponível em:

<http://jus.uol.com.br/revista/texto/857/recurso-especial-e-recurso-extraordinario-concessao-do-efeito-suspensivo-possibilidade>. Acesso em: 12 ago. 2020.

ARTIGO19. *Proteção de dados pessoais no Brasil – Análise dos projetos de lei em tramitação no Congresso Nacional*. Disponível em: <<http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>>. Acesso em: 01 de set. 2020

AZEVEDO, Ana Cristina Carvalho. *Marco civil da internet no Brasil: análise da Lei 12,965/14 e do direito de informação*. Brasília: Alta Books, 2014.

BRASIL. Constituição(1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado, 1988.

BRASIL, Lei nº. 5.869. *Código de Processo Civil*. Brasília, 11 de janeiro de 1973.

BRASIL. LGPD (2018). *Lei Geral de Proteção de Dados*.

BRASIL. *Lei Nº 13.709, De 14 De Agosto De 2018*. Brasília, DF: Casa Civil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 30 ago. 2020.

BRASIL. *PL 5.276, De 13 De Maio De 2016*. Brasília, DF: Poder Executivo. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 27 ago. 2020.

Brasil. *Quem vai regular a LGPD?* Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>. Acesso em: 10.set.2020.

BRASIL. [Lei nº 13.853]. *Lei nº 13.853, de 8 de julho de 2019*. Brasília, DF: Presidência da República, [2019]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Constituicao/Constituicao.htm](http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm). Acesso em: 1 set. 2020.

BOND, Robert. *A 61-million-person experiment in social influence and political mobilization*. 2012. Political Science Department, University of California, San Diego; Psychology Department, University of California, San Diego; Data

Science, Facebook, Inc., Menlo Park; Medical Genetics Division, University of California, San Diego, 2012.

CLEMENT, James. *Number of monthly active Facebook users worldwide as of 2nd quarter 2020*. Disponível em: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> Acesso em: 13.set.2020.

COUNCIL OF EUROPE. *Protection of personal data and privacy*. Disponível em: <https://www.coe.int/en/web/portal/personal-data-protection-and-privacy>. Acesso em: 1 set.2020.

DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Livraria RT, 2006.

ESTEVEZ, Adriana Costa. *A lei cibernética precisa “evoluir muito” e aumentar as sanções, diz ex-Interpol*. Disponível em: <https://www.zeddbrasil.com/a-lei-cibernetica-precisa-evoluir-muito-e-aumentar-as-sancoes-diz-ex-interpol-22-07-2020/>. Acesso em: 25.ago.2020.

EUROPEAN UNION. *Data protection and online privacy*. Disponível em: [https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index\\_en.html](https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.html). Acesso em: 27.jun.2020.

FOUCAULT, Michael. *Michel Foucault on the Panopticon Effect*. Disponível em: <https://fs.blog/2014/07/the-panopticon-effect/>. Acesso em: 15 set.2020.

MAYER-SCHÖNBERGER, Victor; CUKIER; Kenneth. *Big Data. Como Extrair Volume, Variedade, Velocidade e Valor da Avalanche de Informação Cotidiana*. Brasília: Alta Books, 2013.

MENDES, Laura Schertel. *Privacidade, proteção de dados e a defesa do consumidor*

NETO, Alécio Cantelle. *Marco civil da internet e proteção de dados pessoais* Conteudo Juridico, Brasilia-DF: 17 jun 2020. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/50248/marco-civil-da-internet-e-protecao-de-dados-pessoais>. Acesso em: 17 jun 2020.

PASSARELLI, Vinícius. *O que é LGPD: entenda a Lei Geral de Proteção de Dados*. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/> Acesso em: 13.set.2020.

PETTERS, Jeff. *Data Privacy Guide: Definitions, Explanations and Legislation*. Disponível em: <https://www.varonis.com/blog/data-privacy/>. Acesso em: 15.set.2020.

PONTIERI, Alexandre. *Marco civil da internet - Neutralidade de rede e liberdade de expressão*, Brasília-DF: 17 jun 2020. Disponível em: <https://www.migalhas.com.br/depeso/284816/marco-civil-da-internet-neutralidade-de-rede-e-liberdade-de-expressao>. Acesso em: 17 jun 2020

RODRIGUEZ, Daniel Piñeiro. *O direito fundamental à proteção de dados pessoais : as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação*. 2010. 14 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010.

SWEENEY, Latanya. *Simple Demographics Often Identify People Uniquely*. 2000. Privacy Working Paper 3 - School of Public Policy and Management, Carnegie Mellon University, Pittsburgh, 2000.

WIKIPÉDIA. *Autoridade Nacional de Proteção de Dados*. Disponível em: [https://pt.wikipedia.org/wiki/Autoridade\\_Nacional\\_de\\_Prote%C3%A7%C3%A3o\\_de\\_Dados](https://pt.wikipedia.org/wiki/Autoridade_Nacional_de_Prote%C3%A7%C3%A3o_de_Dados). Acesso em: 6.set.2020.

WIKIPÉDIA. *Facebook–Cambridge Analytica data scandal*. Disponível em: [https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge\\_Analytica\\_data\\_scandal](https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal). Acesso em: 6.set.2020

WIKIPÉDIA. *Panopticon*. Disponível em: <https://en.wikipedia.org/wiki/Panopticon>. Acesso em: 15.set.2020.

XAVIER, Luiz Gustavo. *Para Maia, Autoridade Nacional de Proteção de Dados deveria ser independente do governo*. Disponível em: <https://www.camara.leg.br/noticias/690746-para-maia-autoridade-nacional-de-protecao-de-dados-deveria-ser-independente-do-governo/> Acesso em: 10.set.2020.

YOUYOU, Wu. *Computer-based personality judgments are more accurate than those made by humans*. 2014. Department of Psychology, University of Cambridge and Cambridge Department of Computer Science, Stanford University, Stanford, 2014.