Centro Universitário De Brasília – UniCEUB
Faculdade De Ciências Jurídicas E Sociais – FAJS
Curso de Bacharelado em Direito

THALYTA SOARES DE FARIAS

PRIVACIDADE, MONETIZAÇÃO DE DADOS PESSOAIS E A LGPD: desafios e impactos da Lei nº 13.709/2018.

BRASÍLIA
2020

THALYTA SOARES DE FARIAS

PRIVACIDADE, MONETIZAÇÃO DE DADOS PESSOAIS E A LGPD: desafios e impactos da Lei nº 13.709/2018.

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Prof. Humberto Cunha dos Santos.

BRASÍLIA
2020

DE FARIAS, Thalyta Soares.

PRIVACIDADE, MONETIZAÇÃO DE DADOS PESSOAIS E A LGPD: desafios e impactos da Lei nº 13.709/2018.

63 fls.

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Prof. Humberto Cunha dos Santos.

THALYTA SOARES DE FARIAS

PRIVACIDADE, MONETIZAÇÃO DE DADOS PESSOAIS E A LGPD: desafios e impactos da Lei nº 13.709/2018

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Prof. Humberto Cunha dos Santos.

BRASÍLIA, ____ DE _____ DE 2020.

BANCA AVALIADORA

_____

Professor Orientador

_____

Professor(a) Avaliador(a)

AGRADECIMENTOS

Agradeço primeiramente a Deus que tem me guiado por toda a vida e me permitiu alcançar essa vitória.

Agradeço e dedico esse trabalho de conclusão de curso aos meus pais, Agna e Ado, que apostaram no meu potencial, me amaram incondicionalmente e me ensinaram valores que nenhuma graduação seria capaz de lecionar.

Agradeço ao meu amor, Kairo Felipe, por ter sido meu porto seguro em meio as tormentas e angustias que se afloraram.

E agradeço aos meus orientadores Prof. Humberto Cunha e Fabrício da Mota, por cada dose de paciência e estímulo que dispenderam comigo nesse caminho de desenvolvimento intelectual.

Tenham a minha gratidão como a mínima gentileza dedicada àqueles que me ajudaram a ir além dos meus próprios limites.

Quanto à "morte do anonimato" por cortesia da internet... Submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca. Ou talvez, ainda, a pressão no sentido de levar nossa autonomia pessoal para o matadouro seja tão poderosa, tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e resolutos estejam preparados para a tentativa séria de resistir (BAUMAN, 2014, p. 35-36).

RESUMO

Esse trabalho tem por objetivo retratar o contexto social de criação da Lei nº 13.709/2018, que dispõe sobre a proteção de dados pessoais no Brasil e, sem a intenção de esgotar o assunto, explorar alguns dos desafios a serem enfrentados pela lei que ainda entrará em vigor. Nesse sentido, o direito a privacidade passa por um momento de redefinição jurídica e regulação estatal. A inovação tecnológica tem sido utilizada nos setores públicos e privados para a captação massiva de dados pessoais. A economia de dados, desenvolvida pela sociedade informacional, utiliza algoritmos e tratamento em informações pessoais com a intenção de direcionar decisões políticas, econômicas e sociais. Essa conduta ocorre mediante a violação de direitos fundamentais tais como a liberdade, igualdade, privacidade e autodeterminação informativa do titular. A Lei Geral de Proteção de Dados surge em meio a uma discussão global sobre o tema proteção de dados pessoais, e, influenciado pelo Regulamento Europeu, reconhece a vulnerabilidade dos indivíduos quanto a disposição de seus dados pessoais. O trabalho se dedica, ainda, a analisar a eficácia dos princípios estabelecidos pela norma no processo de tratamento de dados pessoais, a mitigação do instituto do consentimento, os desafios e atribuições da autoridade fiscalizadora e a adequação dos setores públicos e privados às novas regras.

Palavras-chave: Sociedade informacional. Proteção de dados pessoais. Metrô. Capitalismo de vigilância. Economia de atenção. Transparência. Privacidade. Direitos Fundamentais. Vazamento de dados. Publicidade comportamental. Lei Geral de Proteção de Dados. GDPR. Tecnologia.

SUMÁRIO

INTRODUÇÃO

É mediante intensa pesquisa e análise das obras de estudiosos das áreas de direito, economia e ciência da computação, que o presente trabalho se propõe a relacionar a disposição de dados pessoais, a manipulação e predição comportamental e a incidência da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), demonstrando os desafios a serem enfrentados num contexto social tão complexo e dinâmico.

O tema compõe o ramo do direito civil cujo desenvolvimento ocorre de maneira acelerada com o advento de novas tecnologias e das transformações sociais. Essas transformações, porém, precisam ser acompanhadas de reflexão correspondente sobre as questões éticas e jurídicas envolvidas. Nesse sentido, a relevância da proteção de dados pessoais no Brasil pode ser facilmente vislumbrada com as estatísticas abaixo:

> Em 2016, a Internet era utilizada em 69,3% dos domicílios permanentes do País e este percentual aumentou para 74,9%, em 2017. O crescimento da utilização da Internet nos domicílios da área rural foi mais acentuado que nos da área urbana, contribuindo para reduzir a grande diferença entre os resultados destas duas áreas. Em área urbana, o percentual de domicílios em que a Internet era utilizava estava em 75,0%, em 2016, e aumentou para 80,1%, em 2017, e, em área rural, subiu de 33,6% para 41,0%. O mesmo tipo de evolução foi observado em todas as Grandes Regiões (IBGE, 2017).

Com isso, o trabalho divide-se em 5 capítulos sendo o primeiro reservado à análise da transformação social moderna para uma sociedade informacional, onde a conectividade e a inovação tecnológica revolucionaram o modo de fazer negócios, de se relacionar, os valores éticos e até o conceito de privacidade. Explica essas transformações com a ajuda do panoptismo, desenvolvido por Foucault e Bentham, traçando a sua aplicação no contexto atual.

O capítulo 2 se encarrega de conceituar termos essenciais para a compreensão de como a personalidade do indivíduo estende-se ao meio virtual, justificando, assim, a tutela jurídica de direitos fundamentais prevista desde a Carta Magna até a Lei Geral de Proteção de Dados, daqui em diante intitulada LGPD.

No capítulo 3 será minuciado o paradoxo da captação de informações por usuários da rede como moeda de troca para utilização de determinado bem ou serviço, de modo a inaugurar o caráter monetário dos dados pessoais. Contém, ainda, um subtópico exclusivo para a compreensão do funcionamento do mercado de dados.

No quarto capítulo tem-se o núcleo do trabalho onde adentra-se no viés jurídico das tensões suscitadas anteriormente, traçando a linha de evolução normativa no que concerne aos direitos fundamentais inerentes a proteção de dados pessoais, aos princípios que regem a tutela de proteção, as legislações anteriores que serviram de amparo jurisdicional e a regulação europeia que impulsionou o debate nacional resultando na criação da LGPD.

Por fim, no capítulo 5 o trabalho alcança seu auge submetendo a Lei Geral de Proteção de Dados a um escrutínio crítico, suscitando as prováveis adversidades e limitações que a norma enfrentará para alcance de sua completa eficácia.

O tema será abordado de maneira metodológica, com o intuito de demonstrar que além do necessário rigor normativo, há uma carência de ética e justiça no tratamento de dados como meras estatísticas, o que tende a definir padrões de consumo, de controle, influenciar consciências, retirar a liberdade de escolha do indivíduo e definir padrões discriminatórios, mediante a ameaça e violação dos direitos fundamentais como a privacidade, a intimidade e a liberdade.

1 SOCIEDADE INFORMACIONAL

O ser-humano, como animal extremamente adaptável e evolutivo que é, passou por diversas revoluções em busca de aprimoramento do seu eu-consciente. Momentos cruciais acarretaram mudanças de comportamento, destino e crença da raça humana, até o presente marco extraordinário onde indivíduos são considerados *chips* compartilhadores de informações inseridos em uma grande rede (HARARI, 2000).

Indícios dessa transformação apareceram ainda na sociedade pré-industrial:

> A documentação acerca das relações pessoais era restrita a uma pequena parte da vida das pessoas, e isso ocorria dentro de uma elite reinante. A rotina diária das pessoas comuns não era documentada de forma escrita. Isto por ser extremamente fácil conseguir coletar, havendo necessidade, todos os tipos de dados possíveis destes cidadãos, tendo em vista que a maioria das relações pessoais se dava proximamente. Relações negociais eram seladas por aperto de mão e testemunhadas por outros (SCAAR, 2011).

Com o decorrer do tempo relações complexas e confusas tomou o lugar das relações “boca a boca”. Consequência dessa perda de confiança foi a diminuição das relações pessoais e o estabelecimento de relações racionais, dando início ao armazenamento de informações de maneira documentada. Adiante, o modelo de produção industrial impulsionou a consolidação do registro dos fatos e acontecimentos diários como forma de colher evidências. Foi esse processo inicial, do ponto de visto do armazenamento, documentação e uso de informações pessoais, que deu início a formação da sociedade informacional como a conhecemos hoje.

Houve a época em que um computador era concebido como uma máquina imensa e de difícil compreensão e manuseio. Com a chegada dos “computadores pessoais” no mercado, entre os anos 80 e 90, a internet se propagou até tornar-se indispensável. Essa evolução tecnológica e sua acessibilidade impactou tanto a sociedade que, atualmente, um smartphone tem mais de 100.000 vezes o poder de processamento do computador empregado no Apollo 11, utilizado para a ida do homem à Lua 50 anos atrás (GNIPPER, 2019).

Essa integração do computador como objeto pessoal despertou o processo de armazenamento e análises dos dados relativos à vida pessoal de terceiros. Quando

setores econômicos e o próprio Estado conscientizaram-se da utilidade que poderia ter a coleta e armazenamento de informações pessoais de terceiros, iniciou-se o processo de panoptização social.

1.1 Panoptização social

O Panoptismo de Foucault (2014), inspirando por Jeremy Bentham[1], foi desenvolvido na década de 1970 e detalha o padrão da sociedade contemporânea através das novas técnicas de vigilância desenvolvidas para essa mesma sociedade. Para Foucault o Panóptico é como a tecnologia de vigilância e controle se comporta, permitindo uma visão privilegiada das ações e comportamentos daqueles que são monitorados. Nesse modelo de monitoramento denominado “panoptismo” inverte-se o espetáculo, “ao invés de a multidão assistir ao que acontece com uns poucos, são uns poucos que assistem ao que acontece com a multidão” (VEIGA, 2019).

O resultado mais previsível dessa concentração de poder é a capacidade de influência no comportamento dos homens; o domínio onde quer que esse poder seja exercido (FOUCAULT, 2005, p.169). Sob essa ótica, Foucault indica que o principal objetivo desse monitoramento são os aspectos econômicas, visto que o controle sob um grande número de pessoas é exercido por uns poucos observadores. Portanto, “o panoptismo representa a base do poder-saber, que regula a vida dos indivíduos e se constitui no protótipo dos sistemas sociais de controle e vigilância (total), presentes na atualidade” (OLIVEIRA; CARNEIRO, 2016).

No caso do panoptismo social que as tecnologias e plataformas criaram, há um fator distintivo em que o indivíduo se permite ser persuadido, não mais pelos argumentos, mas pelo contexto da submissão em que é praticamente conduzido à aceitação (OLIVEIRA; CARNEIRO, 2016):

> No contexto contemporâneo, essa vontade de controle se presentifica pela recorrente busca por uma sensação de mais segurança, de permanente vigilância e maior visibilidade. Há nisso, contudo, uma

[1] Pan-óptico é um termo utilizado para designar uma penitenciária ideal, concebida pelo filósofo e jurista inglês Jeremy Bentham em 1785, que permite a um único vigilante observar todos os prisioneiros, sem que estes possam saber se estão ou não sendo observados. O medo e o receio de não saberem se estão a ser observados leva-os a adotar o comportamento desejado pelo vigilante. Disponível em: https://pt.wikipedia.org/wiki/Pan-%C3%B3ptico. Acesso em: 20 abr. 2020.

> contradição interna, que se traduz pela paradoxal exposição pública do indivíduo diante dos mecanismos digitais de comunicação e nas redes sociais de compartilhamento de informações pessoais. Há um escambo de “privacidades” no espaço público, em um movimento que promove a publicidade das intimidades. As redes sociais representam o mais atual modelo panóptico, enquanto o panoptismo se constitui na proliferação de dispositivos digitais que, em nome da conectividade, da formação de ‘networks’, que replicam as informações pessoais nos ambientes virtuais (OLIVEIRA; CARNEIRO, 2016, p. 215).

O panoptismo exercido através da internet alcança dimensões inconcebíveis à cognição que dela se utilizam. Foucault advertiu sobre a capacidade de adaptação a cada contexto que os modelos de vigília possuem, utilizando-se de aparência inocente, mas suspeita; as tecnologias obedecem à economias de mercado que possuem seus próprios interesses (FOUCAULT, 2005, p. 120). Nas palavras de Oliveira e Carneiro (2018):

> Enquanto no “panoptismo tradicional”, a pessoa é monitorada a contragosto, embora tenha a sua integridade (teoricamente) assegurada pelo agente monitorador, no contexto das tecnologias da informação, as pessoas agem de modo deliberado, voluntariamente oferecendo suas informações pessoais, vulnerabilizando a sua integridade que passa a ser passível de manipulação pelo(s) agente(s) responsável(is) pelo seu monitoramento.

Assim, a privacidade é desprezada em detrimento da sensação de segurança possibilitando novas formas de dominação, escondidos sob valores supostamente universais.

Com o advento da 4ª Revolução Industrial (SCHWAB, 2019) a inteligência artificial (IA), a robótica e a internet das coisas (IoT, sigla em inglês) tornaram a cultura do monitoramento ainda mais presente, mesmo que a intenção seja negada e até desacreditava por muitos. Somado ao fato de que a sociedade passou a compartilhar uma quantidade de informações sem precedentes em uma conexão global.

E é nessa sociedade informacional (ou sociedade em rede), cunhado por Manuel Castells (2002), que se vive cada dia em uma realidade mais permeada pela tecnologia, conectada e interligada, com uma produção de dados e informações de quantidades incomensuráveis.

Em termos realísticos, a evolução mercadológica e tecnológica não deixa espaço para uma vida austera em isolamento. Com isso, importa ressaltar que o

presente trabalho não se dedica ao combate desses setores, mas sim à falta de transparência e de informações das instituições públicas e privadas em relação aos titulares dos dados.

Vale dizer que não parece razoável exigir tanto dos indivíduos e tão pouco de organizações que ocultam a finalidade e o modo de utilização das informações que estão em sua posse. O resultado disso é a coleta e o uso de dados pessoais como matéria prima para a manipulação de comportamentos, nutrição do falso sentimento de liberdade e a invasão da privacidade.

Dito isso, entende-se que até certo ponto histórico a tutela jurídica do direito à privacidade, liberdade e igualdade foi suficiente. Hoje, dadas as situações descritas, evidencia-se a necessidade de estabelecer novos limites, agora adequados à realidade de uma sociedade informacional. E é nessa visão prospectiva que se faz essencial o estudo do tema da proteção dos dados pessoais.

2 DADOS PESSOAIS E DADOS SENSÍVEIS

Feitas as premissas iniciais do capítulo 1, é necessário conceituar os termos essenciais para a compreensão de como a personalidade do indivíduo estende-se ao meio virtual através de seus dados pessoais.

Nesse sentido, a nova Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) define os seguintes termos (BRASIL, 2018):

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

Doutrinariamente, Maria Luciana Pereira de Souza[2] em sua tese de mestrado (SOUZA, 2018, p. 76), designa dado pessoal como qualquer informação de qualquer natureza, registrada em qualquer modalidade de suporte, relacionada à uma pessoa identificada ou identificável.

A partir disso, a diversidade de informações que evolve cada usuário da rede pode ser dividida em duas categorias: dados pessoais e dados pessoais sensíveis, sendo estes dotados de proteção especial e sigilo.

---

[2] Mestre em direito Direitos Fundamentais e Novos Direitos pela Universidade Estácio de Sá (RJ) Ciência de Dados Aplicada ao Direito pela Pontifícia Universidade Católica do Rio de Janeiro.

A LGPD compreende dados sensíveis como todo e qualquer “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, informação referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”, conforme a figura 1. O que justifica a necessidade de proteção especial aplicada a essas informações.

Figura 1 – Dados Pessoais e Dados Pessoais Sensíveis (RENASCENÇA, 2018).

O caráter sigiloso e confidencial dos dados sensíveis gera preocupação sobre os aspectos legais e éticos dessas informações quanto ao seu vazamento, armazenamento e segurança. A Comissão Europeia (2018, p. 2) destaca que os referidos dados somente poderão ser coletados e utilizados em condições específicas, a exemplo de consentimento explícito ou quando permitido pela legislação nacional, conforme explicará o capítulo 6.

Outrossim, é necessário diferenciar que a incidência de dados sensíveis em dados pessoais não significa necessariamente que todos os dados sensíveis serão pessoais, e que mesmo as pessoas jurídicas e até o governo possuem proteção em relação a esses dados sensíveis, conforme explica Vignoli, Richele e Vechiato, Fernando (2019):

> Existe a iminência de Dados Sensíveis em Dados Pessoais, no entanto nem todo Dado Pessoal é sensível e, tampouco, nem todo Dado Sensível é pessoal. Nesta relação, se faz necessário o esclarecimento de que Dados Sensíveis tanto ocorrem por meio de

> dados de pessoas naturais, quanto de pessoais jurídicas (VIGNOLI; VECHIATO, 2019).

Em contraponto ao previsto na Lei Geral de Proteção de Dados Pessoais (LGPD), os Dados Pessoais, propriamente ditos, passarão a ser considerados sensíveis sempre que expor seu titular a algum tipo de situação constrangedora ou discriminatória, bem como informações sobre remuneração, notas acadêmicas, faturas, dados médicos, acordos conjugais, declaração de imposto de renda. Percebe-se, desse modo, a atribuição de um caráter extensivo à lei desde antes da sua vigência.

2.1 Big Data e Big Analytics

Pois bem, explicada a definição inicial de dados pessoais, passa-se ao próximo passo que é a possibilidade de assimilá-los à matéria prima para um produto muito mais valioso no âmbito comercial: a informação.

Nesse sentido, informações são dados pessoais devidamente tratados, e quando tratada a informação transforma-se em conhecimento, conforme expõe Ana Frazão (2018):

> Para entender a importância do *big data* para a concorrência, é importante entendermos que os dados se diferenciam da informação e do conhecimento. Colocada a questão de forma bastante simplificada, os dados podem ser considerados como matérias-primas da informação e a informação pode ser considerada importante matéria-prima do conhecimento, visto este como o resultado de uma reflexão mais consistente – e preferencialmente suscetível de aplicação – a respeito de informações sobre determinada área ou assunto.

O termo *Big Data* refere-se ao grande volume de dados brutos, não agregados, não organizados, gerados em alta velocidade e variedade, que necessitam de tratamento para serem valorados, organizados e armazenados.

O *big analytics* é o processo de análise e transformação do *big data* com o objetivo de encontrar padrões e tirar conclusões sobre a informação. O tratamento é realizado por computadores, podendo ser agrupados, lidos, convertidos, analisados

com técnicas estatísticas, algorítmicas[3] (DOMINGOS, 2019) e computacionais, a fim de se permitir melhor compreensão para a tomada de decisão e automação de processos.

A partir daí extrai-se um novo tipo de conhecimento denominado de *Data Insight*, a análise do comportamento do usuário cujo resultado que é capaz de influir em decisões importantes de um mercado ou até a criação de Produtos Orientado por Dados (*Data-Driven Product)*.

Sem esses instrumentos, de nada adiantaria ter uma infinidade diversificada de volume de dados sem que fosse possível transformá-los, rápido e eficientemente, em informações que geram valor de mercado, observa Frazão (2018):

> Os dados precisam, portanto, ser processados e trabalhados para que possam gerar valor. Se tal constatação não afasta a importância em si dos dados isolados ou "crus", tem o importante papel de realçar o fato de que o mero acesso à dados, sem a possibilidade efetiva e eficiente de transformá-los em informação, pode ser insuficiente para a obtenção dos respectivos benefícios econômicos.

Sob esse ângulo, a qualidade do tratamento dos dados torna-se mais importante do que a velocidade com que é realizada, pois definirá seu valor e relevância.

Por tratamento, a LGPD define em seu art. 5º, inc. X como "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" executadas mediante emprego de ferramentas tecnológicas, seja identificando

[3] Algoritmo é uma sequência de instruções que informa ao computador o que ele deve fazer. Todo algoritmo tem uma entrada e uma saída visando determinado objetivo: os dados entram no computador, o algoritmo faz o que precisa com eles, e um resultado é produzido. Já o *machine learning* faz o contrário: entram os dados e o resultado desejado, e é produzido o algoritmo que transforma um no outro. Com o *machine learning*, os computadores escrevem seus próprios programas, logo não precisamos mais fazê-lo.

padrões de comportamento humano, catalogando-as, classificando-as ou etiquetando indivíduos.

Nota-se que a maioria das plataformas digitais relaciona o *big data* e o *big analytics* para seu funcionamento e até existência, na medida em que necessitam ter o maior acesso possível aos dados dos usuários para depois poder convertê-los em informações e, a partir daí, utilizar tais informações em seu próprio negócio, compartilhá-las com parceiros comerciais ou tomar decisões.

Nesse sentido, Renato Opice Blum observa:

> Está acontecendo uma verdadeira revolução nos métodos de organização, registro e utilização de dados e informações pessoais. Imagine-se centralizar e cruzar informações, por exemplo, da administradora de cartões de crédito com as informações bancárias do cliente, as informações em relação a seu patrimônio imobiliário, seus veículos, seu acesso à internet, seus contatos e informações coletados nas mais diversas fontes, seus hábitos de compras, perfil em redes sociais etc. Considere-se os diversos bancos de dados com informações disponíveis na internet. Somente com eles, reunindo os dados em um só lugar, entrelaçando-os fazendo referências recíprocas, cruzando dados, é possível conhecer bastante bem uma pessoa. Imagine-se o tanto a seu respeito que sua administradora de cartão de crédito conhece. A grande novidade da sociedade contemporânea é que as informações pessoais estão sendo colocadas cada vez mais facilmente à disposição de quem quiser (e pagar). Isto está oferecendo condições de se conhecerem demasiadamente qualquer pessoa, podendo distingui-la (para privilegiá-la, mas também para discriminá-la), influir em sua vida, seu cotidiano e suas possibilidades (BLUM; ELIAS, 2011).

A realidade abordada pelo advogado e autor traz à tona preocupações éticas e jurídicas reais. Basicamente, a tecnologia atual, que a cada instante se torna obsoleta face às novas criadas, permite a análise de fartos conjuntos de dados, possibilitando resultados analíticos absolutos e fidedignos sobre a pessoa humana. Nesse aspecto, Souza (2018) complementa:

> Em linhas gerais: um *like*, um compartilhamento, uma interação reativa, um *checkin* com geolocalização, um *download*, um *login*, uma busca, enfim, qualquer ato instrumentalizado na rede mundial de computadores permite o armazenamento e o esquadrinhamento da informação. As expertises de tratamento de dados, fizeram nascer tecnologias, como, o *Big Data*, o *Data Analytics*, o *Business*

> *Intelligence*[4], dentre outras, inclusive as anteriormente citadas, *Machine Learning e Artificial Inteligence* (HOWARD; TONY, 2017, p. 45).

Esse novo cenário demonstra a capacidade de transformação da Internet e da tecnologia na sociedade, levando à reflexão pontos nunca antes imaginados.

É em decorrência desse paradoxo entre a ficção feita realidade e o iminente risco de lesão a princípios fundamentais que o presente trabalho e legisladores de todo o mundo se ocupam da temática proteção de dados pessoais, visando a plena eficácia de uma norma que garanta e proteja a dignidade da pessoa humana, principalmente em relação à liberdade, igualdade, privacidade e autodeterminação informacional.

[4] Business Intelligence, ou simplesmente BI, baseia-se em agrupar informações de diversas fontes e apresentá-las de forma unificada e sob métrica comum, a fim de que indicadores aparentemente distantes façam sentido entre si, nas palavras do idealizador “Uma metodologia pela qual se estabelecem ferramentas para obter, organizar, analisar e prover acesso às informações necessárias aos tomadores de decisão das empresas para analisarem os fenômenos acerca de seus negócios.

3 A MONETIZAÇÃO DE DADOS PESSOAIS

A informação no mundo capitalista assume a posição que o petróleo assumira no início do século passado, e como novo “petróleo” do século XXI, suas jazidas são as bases de dados públicas. Entretanto ela não visa a substituição dos velhos recursos, mas a transformação do modo de produção de riquezas. Nesse aspecto, as linhas de produção agora realizam-se de modo econômico e simples.

Observa-se que, diante da diversidade de tarefas executadas por usuários da rede, apenas um baixo percentual de ferramentas (programas e aplicativos) são efetivamente remunerados pelos que o utilizam, assim os desenvolvedores criaram métodos alternativos de custeio do negócio, como a cobrança de funcionalidade avançadas, a venda de marketing direcionado e a monetização de dados pessoais. Nesse sentido, esclarece Guimarães (2018):

> Essa monetização se dá no âmbito do "*Big data*" — conceito que envolve a captação, armazenamento, processamento e capitalização de dados e informações. Através do tratamento desses dados, é possível aprimorar, por exemplo, a publicidade dirigida, baseada em padrões de acesso e consumo, e até mesmo influir no hábito do usuário da internet, escolhendo o que mostrar e o que não mostrar, capitalizando também em cima disto (e até mesmo influenciando o resultado de processos políticos, como sugerem alguns estudiosos).

Nesse sentido há o processo de coleta e produção de *insights* automatizados, sendo estes o mapeamento dos indicativos possibilitando a definição do perfil do usuário (suas preferências de consumo, gostos pessoais, dentre outros). A partir da produção desse *insight* pode-se alcançar, por exemplo, o aumento da retenção de clientes e diferenciação competitiva.

Acrescido da mudança de comportamento dos consumidores, que desejam não mais serem vistos como números, mas como indivíduos, as propostas personalizadas chamam a atenção.

Através dessa demanda do mercado, muitas empresas se empenham em tornarem-se especialistas na coleta de dados, desenvolvendo, assim, a expertise para descrever de modo fidedigno seus usuários, no que tange a gostos pessoais, opiniões, hábitos de consumo, dentre outras características.

A princípio, essa tratativa era regida apenas pelas políticas de privacidade e os termos de uso das ferramentas e plataformas, porém com falta de transparência/informações por parte das empresas e a negligência dos usuários ao ignorarem os termos de uso, os termos de consentimento tornaram-se eivados de vícios. Com isso nasceu a necessidade de criação de normas legais capazes de garantir a tutela do usuário quanto aos seus direitos.

Nesse sentido, se posicionou Têmis Limberger, para quem:

> A necessidade de proteger o cidadão juridicamente se origina no fato de que os dados possuem um conteúdo econômico, pela possibilidade de sua comercialização. Devido às novas técnicas da informática, a intimidade adquire outro conteúdo, uma vez que se tenta resguardar o cidadão com relação aos dados informatizados. Assim, o indivíduo que confia seus dados deve contar com a tutela jurídica para que estes sejam utilizados corretamente, seja em entidades públicas ou privadas. Os dados traduzem aspectos da personalidade e revelam comportamentos e preferências, permitindo até traçar um perfil psicológico dos indivíduos. Dessa maneira, pode-se destacar hábitos de consumo, que têm grande importância para a propaganda e para o comércio eletrônico. É possível, por meio dessas informações, produzir uma imagem total e pormenorizada da pessoa, que se poderia denominar traços de personalidade, inclusive, na esfera da intimidade. O cidadão se converte no denominado homem de cristal. As novas tecnologias tornam a informação uma riqueza fundamental da sociedade. Os programas interativos criam uma nova mercadoria. O sujeito fornece os dados de uma maneira súbita e espontânea e, por conseguinte, depois que estes são armazenados, esquece-se que os relatou. É necessário, então, construir uma tutela eficaz do consumidor. Os meios de comunicação interativos modificam a capacidade de coleta de dados, instituindo uma comunicação eletrônica contínua e direta entre os gestores dos nossos serviços e os usuários. Portanto, é possível não só um controle de comportamento dos usuários, mas também um conhecimento mais estreito de seus costumes, inclinações, interesses e gostos. Disso deriva a possibilidade de toda uma série de empregos secundários dos dados coletados. A função da intimidade no âmbito informático não é apenas proteger a esfera privada da personalidade, garantindo que um indivíduo não seja incomodado devido à má utilização de seus dados. Pretende-se evitar, outrossim, que o cidadão seja transformado em números, tratado como se fosse uma mercadoria, sem a consideração de seus aspectos subjetivos, desconsiderando-se a sua intimidade (LIMBERGER, 2008, p. 219).

Hoje, dificilmente o indivíduo tem total controle sobre suas informações e características pessoais após inseri-las na rede, consolidando as palavras de Chiara Teffé (2017, p. 122) de que “a velocidade da circulação da informação é inversamente proporcional à capacidade de seu controle, retificação e eliminação.”

Em contrapartida, o nível de consciência dos usuários de redes sobre a entrega deliberada, excessiva e voluntária de seus dados pessoais aumentou, principalmente após marcantes e recentes escândalos sobre má utilização dessas informações por agentes autorizados e não autorizados.

O escândalo marcante envolvendo a *Cambridge Analytics* e o *Facebook* levantou questões acerca da solidez e integridade dos processos eleitorais democráticos das eleições norte-americanas e do *Brexit*, após constatada a má utilização de dados pessoais com objetivo de manipular a opinião pública.

Nesse sentido, o grande problema que envolve a coleta de um número inestimável de dados pessoais diz respeito a maneira como as informações serão protegidas e utilizadas. Alguns sites até deixam clara sua política de privacidade e proteção de informações dos clientes, porém de maneira vaga e superficial, sem detalhamentos sobre por onde passam, modo de armazenamento ou tempo de permanência no banco de dados. Outra falha grave diz respeito a falta de treinamento dos funcionários, sujeitando informações pessoais a perdas e repasses para terceiros não autorizados.

Essa utilização dos dados para fins econômicos - sobretudo em se tratando das redes sociais - desperta, entre os estudiosos do tema, grande preocupação para com a privacidade dos usuários da internet e de seus serviços. Estes dados são colhidos, por muitas vezes, sem o devido consentimento dos usuários, que também desprezam seu destino e finalidade.

Ressalta-se o fato de os dados pessoais de um indivíduo serem plenamente passíveis de disposição. Ciente disso, o *Facebook* desenvolveu um aplicativo ainda em teste, o app *Study*, que converte a disposição de dados pessoais (como aplicativos instalados no aparelho celular, tempo gasto em cada um dos aplicativos, país, modelo do dispositivo e tipo de conexão do participante) em remuneração, na tentativa de juntar o útil (a necessidade de insumos para a plataforma) com o agradável (desejo de auferir renda dos participantes).

Para tanto, a companhia se compromete, mediante termos de uso e privacidade a não divulgar ou revender os dados obtidos, nem coletar informações de

logins ou senhas, mas apenas o necessário para aperfeiçoar o próprio *Facebook* de forma transparente.

Desse exemplo compreende-se que a Lei Geral de Proteção de Dados busca garantir a liberdade do indivíduo em permiti-lo fazer o que quiser com sua privacidade, sem proteger a privacidade contra ele mesmo, ou seja, desde que seja uma decisão livre, voluntária e consentida, todos possuem a liberdade de dispor de seus dados pessoais.

Enquanto o setor privado vive os embates éticos e jurídicos descritos acima, o setor público enfrenta o inevitável atraso em adaptar-se as mudanças sociais e a inovação tecnológica que ocorre constantemente em um espaço não mais físico, mas virtual. Daí surge o caráter desterritorializante do ciberespaço e o consequente enfraquecimento da soberania dos Estados, conforme expõe Pierre Levy:

> De fato, o ciberespaço é desterritorializante por natureza, enquanto o Estado moderno baseia-se, sobretudo, na noção de território. Pela rede, bens informacionais (programas, dados, informações, obras de todos os tipos) podem transitar instantaneamente de um ponto a outro do planeta digital sem serem filtradas por qualquer tipo de alfândega. Os serviços financeiros, médicos, jurídicos, de educação a distância, de aconselhamento, de pesquisa e desenvolvimento, de processamento de dados também podem ser prestados aos "locais" por empresas ou 207 instituições estrangeiras (ou vice-versa) de forma instantânea, eficaz e quase invisível. O Estado perde, assim, o controle sobre uma parte cada vez mais importante dos fluxos econômicos e informacionais trans-fronteiriços. Além disso, as legislações nacionais obviamente só podem ser aplicadas dentro das fronteiras dos Estados. Ora, o ciberespaço possibilita que as leis que dizem respeito à informação e à comunicação (censura, direitos autorais, associações proibidas etc.) sejam contornadas de forma muito simples. De fato, basta que um centro servidor que distribua ou organize a comunicação proibida esteja instalado em qualquer "paraíso de dados", nos antípodas ou do outro lado da fronteira, para estar fora da jurisdição nacional. Como os sujeitos de um Estado podem conectar-se a qualquer servidor do mundo, contanto que tenham um computador ligado à linha telefônica, é como se as leis nacionais que dizem respeito à informação e à comunicação se tornassem inaplicáveis (LEVY, 1999, p. 312).

Na corrida para a modernização do setor público, o governo empenha altos investimentos em tecnologias, a fim de diminuir a insatisfação de uma sociedade dinâmica que lida com um sistema rígido e burocrático, reduzir custos, dar maior transparência aos atos e gastos públicos, melhorar a prestação e qualidade de

serviços públicos e estabelecer um diálogo direto entre cidadãos e a administração pública.

Tais modernizações estatais exemplificam-se com a utilização de *blockchains*[5] para autenticação e emissão de certidões online, criação de portais com informações relevantes, ensino a distancia, consulto online ao imposto de renda etc.

Porém, essa vasta utilização de tecnologias na gestão e controle de estruturas essenciais implicam na existência de vulnerabilidades, no sentido de haver fragilidades nos sistemas públicos que se descobertas e exploradas por agentes mal-intencionados podem gerar irreparáveis incidentes de segurança.

Atualmente, um ataque cibernético seria capaz de interromper o fornecimento de água ou energia em cidades inteiras, sem excluir a ameaça a rede de transporte aéreo regida integralmente por computadores sujeitos a ataques e falhas (2019). Em suma, quanto mais o governo e seus cidadãos dependem da tecnologia, maior será a sua exposição a ataques de *crackers, hackers* e organizações criminosas, estando suscetíveis aos denominados *cybercrimes* (2020).

Trazendo as informações para o âmbito nacional em termos práticos, tem-se que no governo federal brasileiro, 32% dos serviços são totalmente digitalizados, 39% parcialmente e 29% não estão disponíveis para acesso online, segundo dados parciais de levantamento do Ministério do Planejamento (BRASIL, 2017). Esse aumento de utilização das tecnologias para realização dos serviços públicos deixa dúvidas sobre a capacidade de órgãos governamentais garantirem a privacidade dos cidadãos, face a morosa ascensão da relevância do tema segurança da informação nos setores privados e públicos.

---

[5] Uma *blockchain* é um tipo de banco de dados que armazena qualquer coisa que tenha valor digital. Cada nova transação é salva em um bloco que, por sua vez, é adicionado a uma cadeia de registros existentes. Uma *blockchain* típica duplica os dados por uma rede aberta, de modo que todas as pessoas na *blockchain* possam ver suas atualizações simultaneamente e todas as atualizações sejam validadas através de um processo de verificação pública que garante precisão sem a necessidade de uma autoridade central, como um banco. *Blockchain* - o que é e qual sua importância? Disponível em: https://www.sas.com/pt_br/insights/analytics/blockchain.html. Acesso em: 9 mar. 2020.

3.1 Estudo de Caso: Metrô de São Paulo e a N1 TELECON

Nesse sentido, parcerias Público-Privadas preveem autorizações expressas para a coleta de dados que utilizam dados pessoais em publicidade programática, como ocorre no acesso a rede Wi-Fi em São Paulo com parceria da empresa N1 Telecom. Segue trechos extraídos dos Termos & Condições (2017) de uso da rede pública:

> Termos & Condições. O conteúdo deste Portal se destina a oferecer aos usuários da internet um painel institucional, informativo e de relacionamento com a FREEWIFIMETRÔ SP.
> 1.4 Ao usar o Serviço, você será considerado como tendo aceitado estes Termos. Se você não aceitar qualquer um destes Termos, você deve imediatamente parar de usar o Serviço.
> 1.5 Nós podemos alterar estes Termos a qualquer momento. Como você estará vinculado a qualquer alteração a estes Termos, você deve rever estes Termos periodicamente. Ao continuar a usar o Serviço após qualquer alteração desses Termos, você será considerado como tendo aceitado os Termos alterados.
> 2. Uso do Serviço
> 2.1 Antes de usar o serviço, você deve registrar alguns de seus dados conosco, através de uma instalação on-line que nós fornecemos. Depois de ter registrado, seu dispositivo sem fio será reconhecido automaticamente, e você poderá usar o Serviço.
> 3. Consentimento para receber mensagens
> 3.1 Você concorda em nos fornecer um endereço de e-mail válido ou outro método de contato eletrônico que nós especificamos de tempos em tempos, e receber comunicação (“Mensagens”) nossas através desse endereço de e-mail ou outro método de contato. Nós podemos recusar ou suspender o seu acesso ao Serviço se nós identificarmos que o endereço de e-mail ou outro método de contato que você forneceu não é válido.
> 3.2 Exemplos do conteúdo das Mensagens que você pode receber incluem:
> - material para fins promocionais e de marketing, que podem estar relacionados a produtos e serviços oferecidos por nós ou outras pessoas, empresas ou organizações;
> - material para fins de pesquisa e análises; e
> - material para qualquer outra finalidade que nós consideramos como sendo apropriado de tempos em tempos.
> 3.5 Você reconhece que, se você retirar seu consentimento para receber Mensagens, você não poderá mais usar o Serviço.
> 3.6 As Mensagens podem conter promoções, anúncios e ofertas por outras pessoas, empresas ou organizações (“Promoções de Terceiros”). As Promoções de Terceiros não são aprovadas ou recomendadas pela N1 Telecom ou sociedades, diretores, administradores, empregados ou agentes a ela relacionados.

Conforme trechos destacados acima, o meio de financiamento do serviço deixou de ser pecuniário, passando a ser os dados dos usuários. Os tópicos 3.1 e 3.2

evidenciam que a finalidade do recolhimento das informações é o marketing direcionado, que será veiculado via SMS, e-mails ou qualquer outra forma de divulgação.

Logo adiante, o tópico 4.2 exemplifica a obscuridade cujo presente trabalho visa combater em todos os sentidos, mas principalmente ético e normativo. O termo prevê a coleta indiscriminada de informações pessoais de milhares de pessoas, mesmo não sendo estritamente necessárias para a utilização do serviço. Em capítulo posterior será explicado de que maneira empresas se beneficiam da coleta de excedentes manipulando e prevendo comportamentos.

> 4.2 Além das informações que você nos fornece diretamente, nós podemos também coletar informações automaticamente, inclusive sobre seus dispositivos sem fio, quando eles se comunicam com pontos de acesso sem fio (seja quando você está ou não acessando ativamente a internet) e sobre o seu uso do Serviço (incluindo como e para que fins você acessa a internet).

Nesse sentido, a Lei Geral de Proteção de Dados veda ações que visam a coleta de excedente informacional, de modo a fugir do objetivo inicial: o fornecimento do serviço:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> (...)
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

O trecho abaixo confirma a livre coleta de informações, sem que o titular dos dados tenha ciência do que está sendo efetivamente coletado:

> 4.3 Sujeito ao disposto na cláusula 4.4, você explicitamente concorda que nós podemos usar quaisquer informações que nós coletamos sobre você, ou de qualquer dispositivo associado a você, para qualquer finalidade lícita, tais como:
> - fornecimento de material de publicidade e marketing para você, que pode estar relacionado a produtos ou serviços oferecidos por nós ou quaisquer outras pessoas, empresas ou organizações;
> - fornecimento de informações estatísticas para qualquer pessoa ou organização sobre o uso do Serviço;
> - fornecimento de informações estatísticas para Fornecedores e outras pessoas, empresas ou organizações sobre a circulação de pessoas (incluindo você) e dispositivos de comunicação (incluindo seus dispositivos de comunicação); e
> - análise por nós do uso da internet (incluindo o seu uso).
> 4.5 Nós podemos usar quaisquer informações que nós coletamos a qualquer momento, inclusive depois de você parar de usar o Serviço.

Levando em consideração o fluxo de pessoas nas 40 estações de metrô das linhas 1 (azul), 2 (verde) 3 (vermelha) e (5) Lilás da Cidade de São Paulo, onde são prestados os serviços de Wi-Fi, é possível projetar, através da média diária de utilização nos dias úteis de cada linha no ano de 2018, que cerca de 3.800.000 (três milhões e oitocentas mil) pessoas tem diversos dados pessoais coletados e monetizados diariamente em troca da utilização de um serviço que a empresa afirma ser “gratuito”, em sentido pecuniário. O exemplo do Metrô de São Paulo evidencia o caráter monetário dos dados dos usuários (tópico 1.4), capaz de autorizar ou não a utilização da rede WiFi, assim como ocorre na compra de qualquer bem ou serviço.

Outra facilidade é demonstrar a alimentação de um *big data* pela empresa que utilizará essas informações para comércio, que por sua vez será tratado mediante o *big analytics* e se transformará em marketing direcionado, estatísticas ou qualquer outro conhecimento de relevância econômica.

No Termo de Privacidade da empresa fica ainda mais claro que o serviço prestado não é gratuito, mas sim pago em forma de dados pessoais:

> Por que precisamos coletar suas informações pessoais?
> A Skyfii, N1 Telecom fornecem conectividade à Internet em suas instalações, fornecendo o Serviço para você, para tanto coletamos certas informações sobre seu uso do Serviço e comportamento nas instalações, por exemplo sobre como, onde e por quanto tempo você usa o Serviço enquanto estiver nas instalações. **Você pode pensar nisso como uma "troca justa", em que o Provedor fornece (e nós facilitamos o fornecimento) do Serviço para você em troca de sua provisão de certas informações sobre suas atividades e recebimento de determinado conteúdo. Nossa análise de dados**

> **permite que nossos Clientes entendam melhor como você e outros clientes se envolvem em seus negócios e instalações. Em última análise, isso permite que nossos Clientes tornem sua oferta de serviço mais atraente e interessante.**
>
> Como coletamos suas informações pessoais?
>
> Em primeiro lugar, poderá ser-lhe solicitado que nos forneça determinadas informações pessoais quando se registar como utilizador do Serviço. Nesse momento, nós (ou nossos Clientes) iremos notificá-lo de que suas informações pessoais estão sendo coletadas. Nós também coletaremos informações pessoais sobre você enquanto você receber e usar o Serviço, por exemplo, seu histórico de navegação enquanto estiver nas instalações do Cliente. **Na maioria dos casos, você não saberá que nós (ou nosso Cliente) estamos coletando essa segunda camada de informações pessoais como ocorre automaticamente em segundo plano**.
>
> Os produtos e serviços que fornecemos aos nossos Clientes podem incluir os serviços de marketing discutidos abaixo, bem como a análise de dados sobre suas atividades em suas instalações (por exemplo, **sua localização e histórico de navegação do dispositivo**).
>
> Publicidade e Marketing
>
> Como mencionado acima, você pode pensar na provisão do Serviço por nossos Clientes como uma troca justa de certas coisas que você fornece ou concorda em receber. Uma dessas "trocas" é o nosso uso de conteúdo publicitário e de marketing, semelhante ao que você pode ter visto em outro lugar (por exemplo, conteúdo de vídeo financiado por anúncios).

Apesar da compensação estabelecida contratualmente entre o Metro de São Paulo e a empresa N1 Telecom fosse a de exploração de conteúdo on-line, é fático que os temos de compromisso são divergentes dos previstos pelo próprio Metrô, quando o serviço foi divulgado.

A publicação previa que os dados seriam de propriedade única e exclusiva do Metrô e que as mesmas seriam mantidas apenas enquanto houvesse a prestação do serviço, porém a empresa, conforme tópico 4.5, utilizaram de procedimento discricionário, sem qualquer prazo de validade, mesmo deixando o usuário de utilizar o serviço.

O caso do Metrô de São Paulo é só um dos vários exemplos concretos em que se deve discutir sobre tecnologia e direito, sobre a opacidade do uso de informações pessoais e a obsessão de grupos pela catalogação de indivíduos e seus comportamentos, como será explicado no próximo capítulo.

3.2 A economia de atenção e o capitalismo de vigilância

Com o advento da Internet em escala global, economias, valores e sociedades inteiras foram transformadas. Quanto ao tema privacidade, antes vista como “o direito de ser deixado só”, essa transformou-se drasticamente, frente ao surgimento de um novo meio social que visualiza a extensão de sua privacidade para o meio virtual, tendo sido, portanto, redefinida como a possibilidade de cada indivíduo controlar o uso de informações que lhe dizem respeito.

Por isso deve-se levar em consideração o controle exercido por grupos econômicos baseados na disponibilização de informações. Tal discussão, face a redefinição de privacidade, exige a busca por equilíbrios sócio-políticos mais condizentes aos objetivos e valores de um Estado Democrático de Direito.

Os denominados “capitalismo de vigilância” e “economia de atenção” despertam para a necessidade de criação de fronteiras compatíveis com a realidade digital.

Em uma visão mais ampla, deve o Estado perceber que os indivíduos e a sociedade exigem convivência democrática, transparente e organizada em um sentido completamente distinto ao pensamento obsoleto de 30 anos atrás, e isso inclui a proteção adequada de registros, manipulações e distorções.

Adentrando no tema, a economia de atenção refere-se à “alocação de tempo e atenção das pessoas diante de uma miríade de atividades, negócios e relacionamentos possíveis” nas palavras de Ana Frazão (2018). A preocupação desse novo modelo econômico advém da transformação de necessidades tradicionais para indução de avaliações, escolhas, o que fazer ou adquirir e com quem fazer ou adquirir, de modo a limitar opções do usuário. Como explica Tim Wu:

> A atenção dos usuários tornou-se um dos maiores bens a serem disputados pelos agentes da economia digital. Quanto mais tempo as pessoas passam em determinadas plataformas, mais intensamente estarão submetidas à publicidade e à coleta dos seus dados, assim como mais suscetíveis estarão estratégias que visam influenciar e alterar suas preferências e visões de mundo (FRAZÃO, 2018).

Nesse cenário, atribuímos alta concentração de poder às plataformas na economia digital, na medida em que intermediam de modo eficiente e célere as mais diversas relações. Circunstâncias como essas põem em risco a própria democracia, diante da perda do debate público e a criação de uma “bolha social”, já que os filtros dão aos usuários apenas o que eles querem. Essa seleção é capaz de polarizar opiniões, deixando os usuários suscetíveis a manipulações de todos os tipos e arruinando a legitimidade das instituições democráticas.

Ocorre que, como já foi exposto, para utilização dessas plataformas é necessário a concessão de dados pessoais suficientes para tornar totalmente nítida a personalidade de uma pessoa. É exatamente a potencialidade reveladora que tais informações carregam em sua essência que as tornam perigosas e desejadas, sendo indispensáveis a sua proteção e controle.

Nesse sentido, uma das características mais importante das plataformas digitais é o seu amplo poder de conexão entre usuários, agentes econômicos e governos. Por isso que os maiores detentores de poder econômico na atualidade tratam-se de agentes que exploram plataformas, utilizando o seu poder de conexão e, consequentemente, o potencial de atrair relacionamentos e negócios. Como exemplos podemos citar o *Facebook* conectando pessoas, bens e serviços, a *Amazon* conectando fornecedores e pessoas, a *Airbnb* conectando bens e pessoas, entre outros (FRAZÃO, 2018).

Visto que a tarefa de se conhecer um público alvo é complexa e envolve altos custos de transação, as plataformas sofisticadas como *Google* e *Facebook* se apresentam como um importante nicho para superar essa barreira, através dos dados pessoais em sua posse. Ana Frazão (2018, p. 78) complementa afirmando que:

> São inúmeros os benefícios e eficiências daí decorrentes, pois as plataformas digitais reduzem relevantes custos de transação e agregam valor para os seus usuários, contornando obstáculos que podem dificultar as transações” e oferecendo recursos preciosos para o aperfeiçoamento das combinações. Tais recursos vão desde informações sobre a qualidade do que é ofertado e a reputação dos agentes (de que são exemplos as diversas formas de rating) até recomendações sobre os produtos que correspondam aos gostos e preferências dos consumidores.

Por esse ângulo, como bem afirma a autora, a tecnologia pode estar sendo utilizada contra a nossa própria individualidade, dada a existência de máquinas capazes de conhecer melhor o homem do que ele mesmo, prever suas ações e interações, e até utilizar vulnerabilidades para manipulação de sentimentos, crenças e ideias para os mais diversos fins, inclusive políticos, como ficou demonstrado nas eleições de Donald Trump e do *Brexit*.

A consequência de o poder ser compreendido como a capacidade de influenciar pessoas é que as ameaças da nova economia vão além do desrespeito a privacidade, liberdade e identidade pessoal, alcançando a cidadania e a própria democracia. Nesse novo modelo econômico, os agentes detentores de vastos bancos de dados se posicionam não mais como concorrentes, mas como o próprio mercado, dominando informações sobre seus milhares de usuários.

A autora afirma que o "imperativo de extração" de dados criou uma economia de escala cuja vantagem singular é a capacidade de prever comportamentos individuais que representam um valor que se compra e se vende, conforme expõe o trecho abaixo:

> A primeira onda de produtos preditivos foi impulsionada pelo excedente extraído em larga escala na internet para produzir anúncios on-line "relevantes". A etapa seguinte ocupou-se da qualidade das previsões. Na corrida pela máxima certeza, ficou claro que as melhores previsões deveriam estar o mais perto possível da observação. Ao imperativo da extração somou-se uma segunda exigência econômica: o imperativo da previsão. Este se manifesta primeiramente por economias de escopo. Em uma fase ainda mais ousada que a extração e previsão, está a coleta de dados para aprofundamento, onde para obter previsões comportamentais ainda mais precisas, ou seja, mais lucrativa, é necessário investiga-se particularidades mais íntimas, visando a personalidade, humor, emoções, mentiras e fragilidades dos usuários. Todos os níveis da vida pessoal seriam automaticamente capturados e compactados em um fluxo de dados destinado às linhas de montagem que produzem a certeza. Realizado sob o disfarce da "personalização", grande parte desse trabalho consiste em uma extração intrusiva dos aspectos mais íntimos de nosso cotidiano. À medida que se exacerba a corrida rumo aos lucros gerados pela vigilância, os capitalistas percebem que economias de escopo não bastam. O excedente comportamental deve, sim, ser abundante e variado, mas o modo mais seguro de prever o comportamento é intervir na fonte: moldando-a. Chamo de "economias de ação" os processos inventados para isso: softwares configurados para intervir em situações da vida real sobre pessoas e coisas reais (ZUBOFF, 2019, p. 57).

A autora expõe precisamente a evolução e as novas ambições do tratamento de dados pessoais por grupos cujo interesse diverge do meramente econômico, adentrando no controle social e exploração de predições sobre indivíduos. Para ela, as grandes plataformas utilizam dos dados pessoais que lhe são entregues para monetização em larga e arbitrária escala.

Essas ações em um mundo de economias neoliberais, que não dá o devido valor aos direitos sociais e ao bem-estar social de seus cidadãos, acarretam uma obtenção imoderada de individualidades em dimensões coletivas, desconsiderando características intimas, remodelando comportamentos conforme interesse próprio, e comprometendo os direitos que a princípio deveriam ser protegidos.

4 A PROTEÇÃO DE DADOS PESSOAIS: ORIGEM E DESENVOLVIMENTO

De fato, criações tão revolucionárias e significativas como as redes não poderiam ficar sem reação jurídica adequada. Fato é que a regulação do tema sempre foi motivo de preocupação e sensibilidade no âmbito parlamentar. Hoje, porém, dado o surgimento de conflitos cada vez mais complexos a exemplo dos expostos anteriormente, presencia-se o caso em que a internet, que surgiu predominantemente sem qualquer regulação legal e assim permanecia, agora sofrerá influencias por normas estatais. Nesse sentido explica Michael Kloepfle (SARLET, 2017):

> Ela foi, em grande parte, formada com base nos fundamentos técnicos das redes de telecomunicações que inicialmente eram estatais e que foram privatizadas, bem como daquelas que sempre foram privadas. A organização da rede e a formatação de seu conteúdo é essencialmente um assunto privado, ainda que existam influências estatais que poderão ser reforçadas em virtude da tendência de uma censura estatal da Internet
> Chama a atenção que nela até agora vale o princípio internacionalizado da autorregulação social (ICANN), que, contudo, apresenta déficits democrático. Em virtude dos progressos no que diz respeito ao desenvolvimento de técnicas de filtragem e que criam barreiras de acesso, é de esperar que venha a existir um fortalecimento da influência estatal.

O princípio internacionalizado da autorregulação social (ICANN) ao qual se refere o autor caracteriza-se pelas regras estabelecidas entre os organismos da própria Internet, regulando-se entre si sem interferência externa. Porém esse liberalismo virtual apresenta déficits democráticos, como restou demonstrado no capítulo 3.

Com isso, Estados Democráticos de Direito pelo mundo definiram diretrizes que objetivam cumprir seu dever de proteção dos direitos fundamentais, por entenderem que os dados pessoais constituem uma projeção da personalidade do indivíduo, necessitando inclusive de tutela constitucional. O desafio maior é definir um nível satisfatório de proteção sem deixar de considerar que as ações de terceiros (a

exemplo do direito à livre concorrência e iniciativa[6]) desfrutem de uma proteção com base nos direitos fundamentais que também lhe são inerentes. O Estado então acaba sendo colocado num contexto marcado por expectativas conflitantes por parte de distintos titulares de direitos fundamentais. E como era de se esperar, o fortalecimento da influência estatal se consubstanciou na criação da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados).

Para adentrar no âmbito da norma brasileira de proteção de dados é importante resgatar a definição e relevância dos bens jurídicos por ela tutelados, reconhecidos e protegidos desde a Constituição Federal Brasileira de 1988.

4.1 Constituição Federal de 1988: Direitos Fundamentais e a Dignidade da Pessoa Humana

A Constituição Federal de 1988 incide diretamente no processo de tratamento de dados pessoais, principalmente no que concerne aos direitos fundamentais a privacidade, liberdade, igualdade, autodeterminação informativa, e aos princípios que asseguram uma ordem econômica justa e equilibrada e a dignidade da pessoa humana, como bem ressalta a autora Laura Schertel (2008, p. 119) no trecho abaixo:

> A Constituição é o ordenamento jurídico fundamental do Estado e da sociedade, que constitui e limita os processos de poder. A partir de suas características procedimentais, ela configura um sistema de direitos fundamentais que institucionaliza os pressupostos de comunicação necessários à autodeterminação democrática dos cidadãos. Segundo uma compreensão dinâmica da Constituição, esta constitui um projeto inacabado, sempre sujeito a alterações interpretativas, que refletem um processo de aprendizagem falível.

E é para a perfeita compreensão da abordagem sobre a Lei Geral de Proteção de Dados que o presente trabalho dedicará os próximos subtítulos a breve explicação desses direitos e princípios.

---

[6] A livre concorrência está correlacionada com o princípio da livre iniciativa, ou seja, quando se está diante de um mercado competitivo, os empresários que estejam atuantes com suas atividades, podem perfeitamente utilizar todos os recursos lícitos para que desenvolvam da melhor maneira possível sua atividade econômica. Desta feita, a concorrência permite que o mercado se mantenha com aqueles que são os mais capacitados para fornecer produtos e serviços diferenciados à clientela.

4.1.1 Privacidade

O começo dos debates doutrinários sobre o direito à privacidade ocorreu como consequência da criação de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relativos à vida privada do indivíduo de uma forma anteriormente impensável, remoldando assim o próprio significado desse direito fundamental. Nesse sentido, afirma Laura Schertel (2008, p. 14):

> A origem do direito à privacidade ocorreu em momento diferente de outros direitos de cunho liberal, na medida em que não foi reconhecido nas Constituições, nem nos Códigos Civis do século XIX. Sua origem deu-se inicialmente no contexto doutrinário, tendo sido reconhecido no âmbito legislativo apenas no século XX.

Essa remodelação se deu pelo abandono do dogma anterior, que relacionava a proteção da vida privada à propriedade, pelo novo conceito de proteção à inviolabilidade da personalidade. Nas palavras de Warren e Brandeis “o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas o da inviolabilidade da personalidade” (WARREN; BRANDEIS, 2011).

A partir dessa explicação é possível enxergar o caráter fortemente individualista da proteção à privacidade em suas primícias, com a sua existência reduzida ao direito a ser deixado só (*right to be let alone*) (WARREN; BRANDEIS, 2011). Essa é justamente a causa de sua assimilação a um direito negativo, anteriormente também acompanhado da necessidade de abstenção do Estado na esfera privada individual para a sua concretização.

O século XX foi o período de reinvenção da privacidade onde o Estado, aliado a intensa revolução tecnológica da época e difusão e recolhimento acelerados de informações, passou a considerá-la uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático. A autora elucida esse período com o seguinte trecho:

> Após a II Guerra Mundial, a proteção à privacidade ganha reconhecimento no âmbito internacional. A Declaração Universal dos

> Direitos do Homem, de 1948, prevê, em seu art. XII, além do direito à privacidade, também o direito à honra e ao sigilo de correspondência, nos seguintes termos: “Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques”. A Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos, no Pacto de São José da Costa Rica também previram a proteção da vida privada em termos semelhantes (SCHERTEL, 2017, p. 215).

No contexto constitucional brasileiro, o direito à privacidade é tido como uma espécie de direito à personalidade do indivíduo. Possui tanto caráter negativo (direito de defesa), como de caráter positivo (direito à prestação). A autora explica:

> Negativo, por delimitar uma esfera de proteção, que não pode sofrer intervenção do poder estatal ou privado, exigindo a abstenção do Estado nesse âmbito. Positivo, por ensejar também a obrigatoriedade de uma ação do Estado para garantir tal proteção. Assim, por exemplo, exige-se a intervenção estatal ao determinar a obrigatoriedade de prestar informações pelos órgãos que realizam o tratamento dos dados pessoais (SCHERTEL, 2017, p. 199).

Trazendo para o aspecto prático, o caráter negativo remete a premissa de que nenhuma lei poderá ser promulgada de modo a anular ou eliminar esse direito fundamental, sob pena de vir a ser considerada inconstitucional e ser declarada nula. No tocante do seu caráter positivo, o direito fundamental à proteção de dados pessoais, reconhecido indiretamente pela Constituição, impõe ao Estado deve de agir para proteger a personalidade do indivíduo, tal como a edição de lei específica que regule o assunto.

A Constituição Federal prevê diversas disposições que se relacionam à proteção da privacidade e dos dados pessoais, a exemplo da inviolabilidade da vida privada e da intimidade (art. 5º, X), a vedação da interceptação de ligações telefônicas, telegráficas ou de dados (art. 5º, XII), a proibição da invasão de domicílio (art. 5º, XI) e de correspondência (art. 5º, XII) e a materialização do direito à privacidade: o habeas data (art. 5º, LXXII), um direito fundamental processual para o conhecimento e correção de dados pessoais. Este último, porém, tornou-se ineficaz na proteção de dados pessoais pelo desafio do impetrante em ter exata ciência sobre quem são os

detentores dos dados pessoais, suas finalidades, quais dados são utilizados, de que forma e para qual motivação.

Fato é que a privacidade atualmente enfrenta ofensas que vão além do modelo clássico da invasão e captura indevida de dados pessoais, agora o paradigma da privacidade precisa lidar com os velhos ilícitos, mas também com os métodos lícitos atuais.

Nesse sentido, a teoria dos mosaicos elaborado por Conessa (1984) faz uma construção bastante útil para compreender a privacidade no âmbito dos dados pessoais. A teoria desenvolve que informações inofensivas, quando analisadas isoladamente, se tornam perigosas quando somada a outras, isso por possibilitar a criação de um perfil bastante íntimo e completo de um determinado indivíduo, mas não necessariamente verdadeiro.

Figura 2 – Exemplo da Teoria dos Mosaicos (DANTAS, 2008).

Logo o potencial ofensivo de alguns dados pessoais só é revelado quando relacionado com outras informações. A teoria serve para elucidar as diversas faces da privacidade e demonstra o aspecto macro a ser considerado na coleta de informações pessoais.

4.1.2 Liberdade e igualdade

A existência do Estado está intrinsecamente relacionada a regulação dos indivíduos em todos os seus aspectos e comportamentos, daí o motivo para a classificação de atos lícitos ou ilícitos a todos os atos. A liberdade de tomar decisões, porém, é garantida mediante as variadas formas criadas pelo ordenamento de protege-la.

Numa abordagem rápida, a perspectiva histórico-evolutiva desenvolvida por Mayer-Schonberger (apud. SCHERTEL, 2017, p.36) explica que há três gerações na qual é possível analisar as normas de proteção de dados pessoas sendo a segunda geração de normas de proteção de dados pessoais a que mais nos interessa. Ela refere-se ao paradigma da liberdade:

> A segunda geração de normas de proteção de dados pessoais suscita uma controvérsia bastante interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social. Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca do cadastro de suas informações pessoais.

Nesse sentido, Mayer-Schönberger expõe criticamente o verdadeiro escambo social que o indivíduo tem de realizar para exercer o seu direito à privacidade e à proteção de seus dados:

> A proteção de dados pessoais como liberdade individual pode proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas? Será que nós alcançamos o estágio ótimo da proteção de dados se garantirmos os direitos à privacidade que, quando exercidos, acarretarão a exclusão do indivíduo da sociedade?

A violação da autodeterminação e liberdade do indivíduo se concretiza quando suas informações pessoais, que constituem também a sua personalidade, são

divulgadas indevidamente ou utilizadas sem autorização, acarretando a ausência de controle sobre seus próprios dados pessoais.

A LGPD é medida legislativa que dá ao cidadão os mecanismos necessários para exercer o controle sob suas próprias informações. É também a materialização desse direito fundamental empoderando o indivíduo de determinar o âmbito da própria privacidade impedindo a imposição de uma única visão do mundo (SCHERTEL, 2017).

A autora deixa claro também o sentido da liberdade pretendida no tema dados pessoais, não se constituindo como princípio absoluto, afirma que “ela (a liberdade) articula-se de forma permanente ao princípio da igualdade e ambas compõem em conjunto o preceito da dignidade humana”. Entende-se, portanto, que o exercício pleno da liberdade de controle de dados pessoais baseia-se no consentimento consciente e informado por parte do titular.

Nesse sentido, a LGPD (Lei Geral de Proteção de Dados Pessoais) intenciona munir o indivíduo de livre controle sobre a divulgação e a utilização de seus dados pessoais pelos agentes de tratamento, preservando, dessa forma, a sua capacidade de autodeterminação e de livre desenvolvimento de sua personalidade.

4.1.3 Ordem econômica justa e equilibrada

Certo é que esse princípio envolve vários nichos do direito, mas exclusivamente no âmbito empresa-consumidor a tutela jurídica e a intervenção estatal ocorrem afim de garantir a proteção do consumidor em relação ao mercado que, ao invés de contribuir para a superação da vulnerabilidade do consumidor, vem, na realidade, reforçando essa relação de vulnerabilidade e desequilíbrio, tornando seus consumidores no próprio produto.

Dessa forma, o mercado, principalmente no meio virtual, não pode ser considerado um espaço neutro para escolhas voluntárias e livres, mas sim como um nicho de hierarquias e lucratividade. Daí surge a consciência da inocuidade do “*Laissez faire*”, onde a economia não possui de fato a habilidade de se autorregular sem gerar injustiça.

Conforme mencionado no início desse capítulo para fins de comparação, as redes também seguiam seu próprio sistema de autorregulação (ICANN) e foi mediante essa liberdade que surgiram os mecanismos econômicos e tecnológicos que levam a ofensa dos direitos fundamentais abordados anteriormente.

Daí constatou-se a necessidade de intervenção estatal até mesmo para a manutenção da liberdade e igualdade no mercado de consumo e de dados pessoais. Dada essa breve análise da relevância da regulação do Estado sobre a economia, será feita uma rápida abordagem sobre o diálogo das fontes normativas utilizadas para dirimir os conflitos dobre proteção de dados pessoais de indivíduos.

4.2 Legislação ordinária

Antes da chegada da LGPD algumas legislações infraconstitucionais já se dedicavam na proteção de dados pessoais em seus nichos específicos, a exemplo do Código de Defesa do Consumidor, que estabelece em seu art. 43 a proteção a personalidade e a privacidade do consumidor. Entretanto normas isoladas não foram capazes de alcançar eficácia necessária em todos os seguimentos onde há a utilização ou fornecimento de dados pessoais, como a LGPD se compromete a fazer. Nesse sentido Ruaro, Rodriguez e Finger (2011, p. 12) complementa:

> Integram este rol algumas disposições de natureza comercial e tributária, como o sigilo dos agentes do fisco (art. 198 do CTN), além das Leis n.º 9.296/1996 e n.º 10.217/2001, que tratam da interceptação telefônica e da gravação ambiental. Há, ainda, o Código de Defesa do Consumidor (Lei n.º 8.078/1990), que trata dos bancos de dados nas relações de consumo, bem como a LC 105/2001, que permite às autoridades administrativas a quebra do sigilo bancário, em certas situações, sem autorização judicial.

Também houve a criação da Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckman que inseriu ao Código Penal o artigo 154-A e 154-B, tipificando o crime de invasão de dispositivos para obtenção de vantagem ilícita.

Já a lei 12.527/2011 denominada Lei do Acesso à Informação se dedicou a proteção do direito à privacidade já que ela “determina que o tratamento das informações pessoais detidas por entidades e instituições nela abrangidas seja realizado de modo transparente, respeitando o direito fundamental à proteção da

intimidade, da vida privada, da honra e da imagem" (FORTES, 2016, p. 118), remetendo as informações do indivíduo com os órgãos estatais, alinhada com o disposto da Constituição Federal/88 em seu artigo 5º, inciso XXXIII, artigo 37, parágrafo 3º, inciso II e o artigo 216, parágrafo 2º.

Posteriormente, com a criação da lei 12.965/2014, o Marco Civil da Internet, é que o Brasil iniciou um debate real relacionado a proteção de dados que levasse em conta os novos contornos da privacidade na era digital. O Marco Civil dedicou-se a regulamentar não apenas as práticas e atos na internet, mas também os direitos e garantias dos usuários. Tratou também de temas relacionados aos serviços prestados pelos provedores de internet e sites em geral, e por diversas vezes foi instrumento utilizado para proteção de dados pessoais no que tange a privacidade.

> Mesmo sendo a legislação brasileira considerada pioneira com a promulgação da Lei 12.965/2014, o Marco Civil da Internet (CALIXTO, 2014), pôde se ver um relativo silêncio das autoridades após um primeiro momento, onde se acreditava que a o Marco Civil conseguiria suprir qualquer problemática que poderia ser causada no âmbito virtual, inclusive em relação aos dados pessoais. Ainda assim, mesmo sem uma legislação específica, era visto um esforço por parte do judiciário em manter a preservação dos dados e de sua circulação (BEZERRA, 2019, p. 29).

Nesse sentido, o Marco Civil da Internet pode ser comparado a uma Constituição da Internet, pelo fato de o Marco Civil prever diretrizes e princípios, mas carecer de instrumento sancionador.

4.3 Jurisprudência: realidade da prática jurídica brasileira

No tocante a jurisprudência brasileira, o mundo dos dados trouxe a julgamento casos que exigiram manifestação dos magistrados mesmo na ausência da LGPD. Dessa forma o diálogo entre as fontes normativas supracitadas foi e continuará sendo a base para decisões afim de qualquer violação da proteção de dados pessoais.

A jurisprudência do egrégio Superior Tribunal de Justiça (STJ) concluiu pela existência de um direito de autodeterminação informacional ao afirmar que com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de referência de todo o sistema de

tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem.

Em julgamento do Resp. n. 1348532 / SP, o STJ vetou cláusula abusiva do banco HSBC que obrigava clientes a darem consentimento de repasse de seus dados pessoais para parceiros do banco. O Min. Luís Felipe Salomão da 4ª Turma em seu voto afirma:

> De fato, a partir da exposição de dados de sua vida financeira abre-se leque gigantesco para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se sua maneira de viver e a forma com que seu dinheiro é gasto. Por isso a imprescindibilidade da autorização real e espontânea quanto à exposição. Não bastasse o panorama traçado acima, considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão (BRASIL, 2017).

Analisando o histórico de decisões do STJ no âmbito de dados pessoais e privacidade nota-se que elas se dividem em decisões anteriores e posteriores ao Marco Civil da Internet (Lei nº 12.965/14), e decisões que aplicaram artigos do Código de Defesa do Consumidor e da Lei do Cadastro Positivo. Nesse aspecto, a chegada da LGPD mudará completamente a forma de os magistrados julgarem casos sobre compartilhamento e tratamento de dados.

No âmbito do Supremo Tribunal Federal (STF) tramita o julgamento conjunto da Arguição de Descumprimento de Preceito Fundamental (ADPF) 403, proposta pelo Partido Popular Socialista (PPS) após um juiz do município de Lagarto/SE determinar o bloqueio do aplicativo por 72 horas, e da Ação Direta de Inconstitucionalidade (ADI) 5527, onde ambas ações discutem se há ofensa da liberdade de comunicação por decisão judicial que suspende (em âmbito nacional, mesmo que temporariamente) os serviços de aplicativo de comunicação por mensagem, sendo os dois processos ainda discutidos no momento de escrita do presente trabalho.

Ocorre que argumentos relevantes para o debate do direito a privacidade foram suscitados nos votos já proferidos em 27 e 28/05/2020, não sendo, portanto, dispensáveis as suas análises.

Em ambas as ações, há o questionamento sobre a correta aplicação e interpretação do Marco Civil da Internet (Lei nº 12.965/2014) que permitiria o acesso a mensagens criptografadas ponta-a-ponta[7], mediante ordem judicial. Até o momento os ministros relatores, Edson Fachin e Rosa Weber respectivamente, votaram que autorização a qual a lei se refere seria apenas para a entrega de informações desprotegidas de sigilo, os denominados metadados. O voto do ministro Fachin reforça a inviolabilidade do direito fundamental quando afirma que a proteção da privacidade através da criptografia não é apenas uma proteção ao indivíduo, mas a garantia instrumental do direito à liberdade de expressão (BRASIL, 2020).

Já na visão da ministra Weber, o bloqueio dos serviços de provedores de internet só poderia ser autorizado no caso de as próprias plataformas ofenderem a privacidade do usuário, e não o contrário. Ou seja, o fato de a empresa resistir a uma ordem judicial que pretende justamente essa violação da privacidade não seria justificável para interromper a sua atividade. Isso devido a tutela que o Marco Civil da Internet dá a garantia de privacidade. Por fim, é importante ressaltar a observação da ministra quanto a letra da Constituição que assegura a inviolabilidade do sigilo da correspondência e comunicações telegráficas, de dados e das comunicações telefônicas, exceto por ordem judicial, nas investigações criminais e persecuções penais.

Em resposta a ofício da ADPF 403 solicitando manifestação, a polícia federal se posicionou a favor do fornecimento das informações em prol da segurança pública, haja visto serem dados essenciais para a deflagração de organizações criminosas e casos relevantes, defendendo, ainda a medida de bloqueio da plataforma sustentando a inexistência de violação a preceito fundamental.

---

[7] "A criptografia de ponta a ponta do WhatsApp garante que somente você e a pessoa com quem você está se comunicando podem ler o que é enviado. Ninguém mais terá acesso a elas – nem mesmo o WhatsApp. As suas mensagens estão seguras com cadeados e somente você e a pessoa que as recebe possuem as chaves especiais necessárias para abri-los e ler as mensagens. E, para uma proteção ainda maior, cada mensagem que você envia tem um cadeado e uma chave únicos. Tudo isso acontece automaticamente: não é necessário ativar configurações ou estabelecer conversas secretas especiais para garantir a segurança de suas mensagens. Importante: a criptografia de ponta a ponta está sempre ativada. Não há nenhuma maneira de desativá-la."

Apesar da real obrigação do Governo para com a segurança nacional, a criminalização da criptografia nesse julgamento traria vulnerabilidade ao sistema que protege a privacidade e o sigilo das comunicações dos usuários, conforme alega a defesa do aplicativo *Whatsapp*. O aplicativo também destacou o fato de que a ausência de criptografia na plataforma ou a mera possibilidade de interceptação dos dados que lá circulam teria a consequência óbvia de migração dos criminosos para qualquer dos outros serviços de mensagem totalmente criptografados, deixando a empresa em grave desvantagem concorrencial face aos seus competidores.

Nesse sentido, visto que a LGPD impõe a todas as empresas adequação à sua lista de exigências, é descabido segregar a criptografia desse rol de ações para a segurança das informações, ainda que ela inviabilize ou colida com os interesses da justiça. Logo, a razão das ações deve ser rigorosamente analisada dado que o crime cometido por meio da criptografia não seria justificativa plausível para violação da privacidade de cerca de 120 milhões de cidadãos usuários da plataforma *Whatsapp* (VELOSO, 2017).

4.4 General Data Protection Regulation - GDPR

O Regulamento Geral da Proteção de Dados (*General Data Protection Regulation* - GDPR) - Regulamento 2016/679, trouxe a inovação necessária para área de proteção de dados pessoais. O regulamento implantou conformidade das leis de proteção de dados de todos os países da União Europeia, reconhecendo a preponderância da circulação de dados da sociedade no âmbito das empresas, associações e entes públicos.

O Regulamento reconheceu que o aumento inestimável do fluxo de dados pessoais associado ao desenvolvimento de novas tecnologias e plataformas gerou a necessidade de adaptação e criação de novos princípios capazes de enfrentar a realidade virtual e também real.

Para esse trabalho, porém, a relevância está em demonstrar o efeito dominó gerado pela GDPR em legislações do mundo inteiro, com enfoque na nova Lei Geral de Proteção de Dados brasileira cuja influência de conteúdo e criação se deu preponderantemente pelo regulamento europeu.

O regulamento reforçou a ideia de que sites e empresas, mesmo externos ao território europeu, deveriam seguir suas regras quando utilizadas ou contratadas por cidadãos europeus, além do mais empresas europeias foram vetadas expressamente de continuar negócios com empresas de países que não possuíssem legislação específica para tratamento de dados pessoais. Nesse sentido, as palavras do Min. Luis Felipe Salomão explicam precisamente o princípio da territorialidade das leis relativas à proteção de dados pessoais:

> A comunicação global via computadores pulverizou as fronteiras territoriais e criou um novo mecanismo de comunicação humana, porém não subverteu a possibilidade e a credibilidade da aplicação da lei baseada nas fronteiras geográficas, motivo pelo qual a inexistência de legislação internacional que regulamente a jurisdição no ciberespaço abre a possibilidade de admissão da jurisdição do domicílio dos usuários da internet para a análise e processamento de demandas envolvendo eventuais condutas indevidas realizadas no espaço virtual (BRASIL, 2011).

Ou seja, por mais que o Regulamento Europeu tenha imposto diretrizes a serem seguidas em relação ao tratamento de dados pessoais, isso não retira a liberdade de cada país membro da União Europeia e nem fora dela de criarem suas próprias leis.

Desta forma, a GDPR gerou um efeito cascata no contexto internacional, atingindo o Brasil, impulsionando a criação da LGPD que trata o tema abrangência maior que o Marco Civil da Internet, aprofundando-se em conceitos, regras e sanções mais alinhados com os padrões internacionais.

A intenção do próximo capítulo é, portanto, dedicar-se exclusivamente à análise dos pontos mais importantes dessa lei com um olhar crítico e propositivo, porém sem a menor pretensão de esgotar o assunto, ou mesmo a quantidade de desafios existentes.

5 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018)

A Lei nº 13.709/2018 (LGPD) ainda enfrenta seu extenso período de vacância legal definido pelo art. 65 da lei que estabeleceu o período de 24 meses da data de publicação, ocorrida em 15 de agosto de 2018, para sua entrada em vigor, já os arts. 55 e 58, que dispõem sobre a criação da Autoridade Nacional de Proteção de Dados (ANPD) e seu Conselho, entraram em vigor em 28 de dezembro de 2018. Ainda assim, a 2 meses para o fim do prazo, alguns o julgam insuficiente para adaptação a todas as transformações e adequações exigidas pela norma.

Pode-se dizer que o principal temor dos afetados pela Lei Geral de Proteção de Dados concerne em assegurar os direitos dos titulares, alguns deles inovadores para no ordenamento jurídico e para os setores públicos e privados, a exemplo do direito à portabilidade dos dados pessoais e alguns outros descritos abaixo:

> (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 na Lei;
> (v) portabilidade dos dados a outro fornecedor de serviço ou produto;
> (vi) eliminação dos dados pessoais tratados com o consentimento do titular;
> (vii) informação sobre a possibilidade de não fornecer consentimento e consequências da negativa;
> (viii) revogação do consentimento.

Logo a função da lei não é a de proteger os dados por si só, mas a pessoa que é titular dessas informações. Nesse sentido, percebe-se certa vulnerabilidade do usuário que cede seus dados em troca de bem ou serviço, semelhante ao previsto no Código de Defesa do Consumidor. A diferença crucial é que a proteção prevista na LGPD abrange todos os tipos de dados pessoais em âmbito físico ou virtual, reconhecendo as limitações técnicas, econômicas e jurídicas que indivíduo tem ao lidar com um sistema tão complexo quanto a captação e processamento de dados, muitas vezes encontrando obstáculos intransponíveis para acessar seus dados.

Quanto a sua aplicabilidade e territorialidade, o art. 3, inc. I, II e III da LGPD esclarece que a lei alcançará todos os que realizam qualquer operação de tratamento de dados pessoais, sejam entes públicos ou privados, pessoas físicas ou jurídicas,

independentemente do meio utilizado ou do país de sua sede ou do país onde estejam localizados os dados, desde que (BRASIL, 2018):

> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> III - os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.

Extrai-se dos incisos supracitados o alcance da LGPD, “na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil”, explica Patrícia Pinheiro (2020), e conclui exemplificando que “o dado pessoal tratado por uma empresa de serviço de *cloud computing* que armazene o dado fora do país terá que cumprir as exigências da LGPD”.

Por outro lado, a lei não é aplicável quando o tratamento dos dados for realizado por pessoa física para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos e artísticos e para tratamentos realizados cuja finalidade for segurança pública e defesa nacional, conforme previsto no art. 4°, I, II, III e IV.

Nesse sentido, a autora sugestiona que “o tema da proteção dos dados pessoais teria sido mais bem recepcionado em sede de um tratado internacional, visto que a natureza atual dos fluxos de dados nos negócios é transfronteiriça” (PINHHEIRO, 2020).

A crítica é pertinente dada a globalização crescente e o intenso fluxo de dados internacionais, o que facilitaria o diálogo em caso de violação aos direitos tutelados. Além disso, em seu ponto de vista, a União Europeia alcançou sucesso em conseguir consolidar em um único regulamento geral as diretrizes de 28 Estados-Membros, mediante o GDPR, abrindo precedente para que as demais regiões do planeta fizessem o mesmo conjuntamente.

Contudo, a leitura da LGPD não deixa dúvidas de sua similitude com o GDPR, justamente com a intenção de amenizar as diferenças técnicas, jurídicas e econômicas entre usuários e empresas, públicas ou privadas, internas ou externas ao território brasileiro. Nesse sentido Patrícia (2020) ressalta:

> A versão nacional é mais enxuta e em alguns aspectos deixou margem para interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir espaço para subjetividade onde deveria ter sido mais assertiva. Um exemplo disso ocorre em relação à determinação de prazos: enquanto o GDPR prevê prazos exatos, como de 72 horas, a LGPD prevê "prazo razoável (PINHEIRO, 2020, p. 231).

Uma explicação para essa flexibilidade seria devido aos desafios que a lei representa para todos os setores por ela regulados, conforme será demonstrado ao longo do capítulo.

O artigo 6º se encarrega justamente de apresentar os princípios que regem a norma e que são responsáveis pela harmonia da legislação brasileira com a internacional. Apesar não serem dotados de força normativa, são eles que vão nortear e limitar o tratamento de dados pessoais nos setores públicos e privados para que o indivíduo possa exercer seu poder de autodeterminação informativa:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de

> situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Apesar de ainda não estar em vigor, deseja-se que a LGPD seja capaz de lidar com o desafio da tecnologia e modernidade, tratando a proteção dos dados com o devido respeito e seriedade, reconhecendo a titularidade dos dados de propriedade dos indivíduos, e não das organizações como ocorre em países que não possuem a legislação, norteando o tratamento de dados durante sua captação, armazenamento, processamento, uso e exclusão.

No tocante às penalidades, estão previstas no art. 52 e deverão observar alguns critérios em sua aplicação, especialmente o da proporcionalidade. Dentre as possibilidades de sanções estão: advertência, publicização da infração, suspensão parcial, sanções administrativas e até proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Dentre elas, a que mais se destaca está no inc. II que prevê “multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;”

É importante, ao menos de início, que sejam preferidas as sanções administrativas em detrimento da aplicação de multas rigorosas como essa, isso por que a lei se propõe a estimular a mudança cultural nas organizações de modo que os princípios citados anteriormente se tornem pilares internos. Nesse sentido, o art. 2º esclarece que a lei foi criada não só para o titular dos dados, mas também para o desenvolvimento econômico dos agentes de tratamento de dados.

Entre os aspectos que podem ser considerados na amenização de uma sanção pela Autoridade fiscalizadora estão a gravidade e natureza das infrações e da

categoria dos direitos pessoais atingidos, a boa-fé, reincidência entre outros previsto no art. 52, §2º e incisos.

Sendo assim, um sistema de gestão de dados pessoais bem empreendido pode ser relevante na redução das penas, na hipótese da incorrência em algum tipo de infração que enseje a aplicação de penalidade. É necessário que os setores afetados pela lei reorganizem sua governança corporativa para focar nos princípios que foram previstos pela LGPD, tornando o negócio sustentável.

5.1 O paradigma do consentimento na LGPD

O instituto do consentimento, aplicado ao tema do tratamento e proteção de dados pessoais, apresenta diversas adversidades, como a exclusão do indivíduo do mercado de consumo, e até mesmo da sociedade, na hipótese de negativa de consentimento (SCHERTEL, 2008).

O autor Mayer-Schönberger suscita debate sobre o custo social que o titular dos dados precisa pagar para exercer o seu direito à privacidade e à proteção dos dados pessoais: “Será que nós alcançamos o estágio ótimo da proteção de dados se garantirmos os direitos à privacidade que, quando exercidos, acarretarão a exclusão do indivíduo da sociedade?” (SCHERTEL, 2008, p. 36). Essa indagação é facilmente respondida pelo exemplo do Metrô de São Paulo ao prever a exclusão do indivíduo do acesso a internet devido ao não consentimento de disposição da sua própria privacidade. Segue trecho abaixo:

> Termos & Condições. O conteúdo deste Portal se destina a oferecer aos usuários da internet um painel institucional, informativo e de relacionamento com a FREEWIFIMETRÔ SP.
> 1.4 Ao usar o Serviço, você será considerado como tendo aceitado estes Termos. Se você não aceitar qualquer um destes Termos, você deve imediatamente parar de usar o Serviço. (...)
> 3.5 Você reconhece que, se você retirar seu consentimento para receber Mensagens, você não poderá mais usar o Serviço

É justamente o que o autor Danilo Doneda (2006) denomina como paradoxo da privacidade, dado que nessa antiga estrutura primeiro o direito exigia que o indivíduo autorizasse o processamento de seus dados, para apenas depois poder solicitar a tutela jurídica.

Com a criação da norma de proteção de dados, o instituto do consentimento sofrerá adequação por parte dos setores públicos e privados, tornando-o mais condizente com a realidade de uma sociedade em rede e de informação:

> Art. 5º Para os fins desta Lei, considera-se:
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Com isso, o consentimento passou a ser instrumento da manifestação da vontade individual. “Se por um lado ele revela o aspecto da autodeterminação, já exposto ao longo deste trabalho, também passa a figurar como instrumento de legitimação” (DONEDA, 2006, p. 56).

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

A norma estabelece, então, que o fornecer do consentimento não significa a falta de interesse do indivíduo na tutela de suas informações pessoais, mas sim um ato de escolha garantida pela sua autodeterminação individual.

Sob essa ótica, adquire grande relevância e constitui importante inovação a possibilidade de revogação do mesmo, prevista no art. 8º, §5º da lei. Tal prerrogativa é fundamental para fazer valer os direitos de liberdade e privacidade. Na legislação brasileira, a revogação é válida tanto para autorização para o tratamento, quanto em relação à circulação dos dados:

> Art. 8º. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

A nulidade de autorizações genéricas, prevista no §4º acima, tem grande relevância para a eficácia do consentimento visto que pode configurar vício de vontade. Diferentemente do tratamento previsto no Código Civil para negócios jurídicos defeituosos, a manifestação da vontade com vício de consentimento é anulável, já na LGPD esta mesma manifestação configura nulidade. Nesse sentido, o legislador adotou medida mais extrema pelo fato de que, segundo a LGPD, os dados pessoais são projeções da personalidade.

Todavia, a revogação não impede que o usuário do bem ou serviço não seja excluso da utilização dos mesmos. Importante ainda compreender que mesmo após a revogação do consentimento, as condutas abusivas não estarão isentas de reparação, na hipótese de danos ao titular dos dados. Outrossim, contam com especificidades o consentimento das seguintes categorias de dados e tratamento:

> Dados pessoais sensíveis: quando a base legal for o consentimento, o tratamento de dados pessoais sensíveis somente poderá ocorrer quando o titular ou seu responsável legal autorizar, de forma específica e destacada, para finalidades determinadas.
> Dados pessoais de crianças e de adolescentes: o consentimento deve ser específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal.
> Transferência internacional de dados pessoais: quando também for baseada em consentimento, este deve ser específico e em destaque, com informação prévia sobre o caráter internacional da operação, distinguindo claramente de outras finalidades (BRASIL, 2018).

Com esses ajustes, juntamente com a atuação do encarregado de proteção de dados da organização, e com o trabalho jurídico e técnico adequado, é possível amenizar os riscos de violação da LGPD e, consequentemente, a aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD).

Mesmo com esses gatilhos de mitigação do vício de consentimento, há a realidade do cansaço social em fornecer sua autorização para cada ação tomada. É fato que a exaustão levará novamente ao vício, não podendo a empresa ou órgão ser mais responsabilizado pela negligencia de seus usuários. Daí a importância da consciência social, visto que de nada serve os termos sem uma cultura de compreensão do que são os dados pessoais. Essa consciência ainda está em seus primeiros passos no Brasil.

5.2 Autoridade Nacional de Proteção de Dados (ANPD)

O art. 55, que entrou em vigor em 28 de dezembro de 2018, dedicou-se exclusivamente à criação da Autoridade Nacional de Proteção de Dados (ANPD) como sendo um “órgão da administração pública federal, integrante da Presidência da República” (BRASIL, 2018), com autonomia para a aplicação de penalidades administrativas e pecuniárias aos infratores da LGPD.

Sob essa ótica, existem inúmeros desafios e incertezas que a própria LGPD deixou ao encargo da autoridade. Diferentemente da ANP, ANEEL, ANATEL e demais agências setoriais, a ANPD fiscalizará todos os empreendimentos, organizações e atividades, desde farmácias até as gigantes da tecnologia.

Extrai-se daí que a autoridade deverá articular sua competência com a atuação prévia de outros órgãos reguladores, como o Conselho Administrativo de Defesa Econômica (CADE), a Secretaria Nacional do Consumidor (SENACON) e a Agencia Nacional de Telecomunicações (ANATEL), bem como o diálogo com Autoridades estrangeiras, nas hipóteses de extraterritorialidade.

Existe ainda a preocupação com o aumento do número de judicializações após a entrada da lei em vigor, visto que essa cultura já está impregnada no ideal brasileiro. Esses desafios demonstram que mesmo com a existência da ANPD, o tema da proteção de dados será recorrente no Judiciário, sujeito à carência de maturidade técnica, jurisprudencial e doutrinária, podendo acarretar grande insegurança jurídica. Outrossim, paira a dúvida se a ANPD conseguirá atender às necessidades da legislação e da sociedade, bem como se a estrutura de agência reguladora, no atual contexto, seria a melhor opção.

5.3 Aplicação da lei no setor privado

Como se vê, setores empresariais deverão se empenhar para adequar-se à lei adotando sistema de mapeamento e classificação de informações em sua propriedade, atribuindo o nível correspondente de segurança e restrição de acesso, investindo no treinamento constante de todos os seus dirigentes e colaboradores, conforme requisições da própria LGPD. A previsão é que esta atingirá principalmente

os setores de recursos humanos, hospitais, farmácias e escritórios de advocacia, devido ao grande fluxo e armazenamento de informações de terceiros.

No âmbito virtual privado, práticas como o aceite de termos de uso e políticas de privacidade de difícil compreensão com apenas um clique será alvo da adequação a LGPD, tendo em vista que o consentimento deve ser baseado no aceite de informações compreensíveis e, quando possível, ser solicitado gradualmente de acordo com a necessidade e finalidade.

Já no ramo farmacêutico, dados pessoais como RG, CPF, filiação, telefone e endereço, e dados sensíveis como o estado de saúde do titular deverão ser obedecer rigorosamente aos deveres de tratamento previstos pela LGPD, principalmente relacionado à gestão, sigilo e segurança dessas informações. Outrossim, o hábito de farmácias requisitarem dados pessoais em compras que sequer envolvem medicamentos, como loções, cremes, preservativos, passou a ser é uma modalidade totalmente ilegal.

As redes sociais representam exigem maior cuidado por parte dos usuários das plataformas pois a superexposição não é protegida pela lei. Ou seja, o livre compartilhamento de informações pessoais em redes como *Facebook*, *Instagram* ou *Twitter*, por exemplo, pode acarretar consequências graves cujo consentimento foi legítimo.

Vale dizer que as redes sociais se utilizam da monetização de dados pessoais para permitir acesso às suas plataformas, conforme exposto no capítulo 3. Dessa forma, elas também passarão por adequação da LGPD quando aos termos de uso e política de privacidade para torna-los mais compreensíveis e finalísticos antes que o usuário dê livre acesso a informações de cunho extremamente pessoal como fotos, compromissos e contatos.

Esses são apenas alguns exemplos de setores que serão desafiados pela adequação à LGPD. Por fim é necessário ressaltar que a criação da lei traz consigo uma série de benefícios como a possibilidade do livre fluxo de dados com os países signatários do Regulamento Europeu, aumentando a competitividade das empresas brasileiras e facilitando a internacionalização de iniciativas nacionais.

A elevação da transparência no mercado é outro fator que estimula a confiabilidade de titulares de dados nos mercados adequados a legislação, dado o controle do usuário sobre suas próprias informações, e, por fim, o diferencial significativo em mercados acirrados, onde a organização em *compliance* com a LGPD será mais considerada em detrimento de outra que não demonstra cuidado com os dados de seus clientes. Nesse sentido Felipe Palhares[8] (2018) corrobora:

> Encarar a LGPD como uma oportunidade (ainda que complexa) é muito mais beneficial do que enfrentá-la como um inimigo mortal. Inovar é criar formas novas de resolver problemas ou de superar obstáculos, desde que dentro das regras do jogo. Caso contrário, a inovação se torna ilícita e prejudicial não somente ao malfeitor, mas a todo o mercado. Essa é a única "inovação" que a LGPD vai frear e que, se não fosse ela especificamente, outras leis o fariam. Na verdade, a LGPD tem o potencial de fazer justamente o contrário: impulsionar a inovação responsável e incentivar a criação de modelos de negócio não somente viáveis comercialmente, mas também do ponto de vista da privacidade de seus usuários.

5.4 Aplicação da lei no setor público

Não seria admissível que o próprio Poder Público se esquivasse de uma legislação sobre privacidade e proteção de dados pessoais de seus próprios cidadãos, sendo o Estado o detentor de um *big data* inestimável e o principal agente de tratamento dessas informações. Nesse sentido:

> A aplicação da LGPD ao Poder Público e ao Poder Privado, essencialmente de forma indistinta, ainda que respeitada algumas diferenças, é um grande desafio, que se não for realmente superado, coloca em xeque a *ratio legis* da lei, que é proteger os dados pessoais e a privacidade dos usuários contra abusos e atribuir maior controle do titular dos dados sobre os mesmos, durante toda a cadeia de tratamento, independentemente da natureza da empresa (MIGUEL, 2019).

O caso da parceria público-privada entre o metrô de São Paulo e a empresa N1 Telecom é exemplo claro de violação da LGPD, bem como da imperiosa necessidade de adequação a norma. Diferentemente do previsto nos tópicos 1.4 e 1.5

[8] Sócio fundador do Palhares Advogados, mestre em Corporate Law pela New York University, professor convidado do Insper, primeiro brasileiro a ser reconhecido como Fellow of Information Privacy e o único brasileiro a obter todas as certificações de privacidade e proteção de dados da International Association of Privacy Professionals (CIPP/E, CIPP/US, CIPP/C, CIPP/A, CIPM, CIPT).

do Termo e Condições, o consentimento do usuário não poderá ser deduzido da utilização do serviço, mas deverá ser solicitado gradualmente, conforme estrita necessidade e finalidade informada, nos termos do art. 8, §4º da LGPD que dispoe que “o consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.”

> Termos & Condições. O conteúdo deste Portal se destina a oferecer aos usuários da internet um painel institucional, informativo e de relacionamento com a FREEWIFIMETRÔ SP.
> 1.4 Ao usar o Serviço, você será considerado como tendo aceitado estes Termos. Se você não aceitar qualquer um destes Termos, você deve imediatamente parar de usar o Serviço.
> 1.5 Nós podemos alterar estes Termos a qualquer momento. Como você estará vinculado a qualquer alteração a estes Termos, você deve rever estes Termos periodicamente. Ao continuar a usar o Serviço após qualquer alteração desses Termos, você será considerado como tendo aceitado os Termos alterados.

Outro aspecto comumente encontrado em termos e condições públicos e privados está no tópico 4.2 (cláusula genérica) e 2.1 (coleta indiscriminada de informações pessoais). Nesse sentido, o art. 6 da Lei Geral de Proteção de Dados veda ações que visam a coleta de excedente informacional condicionando-a aos princípios da finalidade e necessidade, a exemplo de adequação necessária com a entrada da norma em vigor.

> 2. Uso do Serviço
> 2.1 Antes de usar o serviço, você deve registrar alguns de seus dados conosco, através de uma instalação on-line que nós fornecemos. Depois de ter registrado, seu dispositivo sem fio será reconhecido automaticamente, e você poderá usar o Serviço.
> (...)
> 4.2 Além das informações que você nos fornece diretamente, nós podemos também coletar informações automaticamente, inclusive sobre seus dispositivos sem fio, quando eles se comunicam com pontos de acesso sem fio (seja quando você está ou não acessando ativamente a internet) e sobre o seu uso do Serviço (incluindo como e para que fins você acessa a internet).
>
> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> (...)

> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

O caso do Metrô de São Paulo é apenas um dos vários exemplos concretos carentes de fiscalização e adequação a LGPD. Em outro aspecto, tem-se o crescente uso da tecnologia na governança pública em escala global, a exemplo da Estônia que possibilitou aos seus cidadãos o acesso a todos os serviços públicos em plataforma online. Utilizando a identidade digital, o indivíduo consegue-se acessar serviços de previdência, agendar uma consulta no sistema de saúde, registra empresas e licenciamentos, transferência de veículos, podendo até mesmo votar de sua residência.

O Brasil também caminha neste sentido da desburocratização, do uso eficiente da tecnologia em prol a eficiência na administração e melhoria da vida do cidadão, mesmo que a passos lentos. Apesar de não ter desenvolvido um documento digital único, já foram disponibilizados documentos como a CNH digital, a carteira de trabalho digital, o título de eleitor digital e o e-CPF, por exemplo. Extrai-se daí a imperiosa necessidade de investimento no setor de segurança da informação e proteção de dados pessoais, para que essas soluções não se torne um problema nacional.

CONCLUSÃO

O mercado evoluiu para a utilização de uma nova moeda de troca: os dados pessoais. É diante dessa disposição massiva de informações que o direito a privacidade enfrenta riscos e novos desafios, a exemplo dos algoritmos. Criados a partir do *big data* e do *big analytics*, os algoritmos inauguraram uma nova economia e uma nova política de tomada de decisões a partir de análises preditivas e marketing direcionado. Nos denominados capitalismo de vigilância e economia de atenção, os agentes detentores de vastos bancos de dados se posicionaram não mais como concorrentes, mas como o próprio mercado, dominando informações sobre seus milhares de usuários.

Nesse cenário, comprovou-se que a predição comportamental e o marketing direcionado são novos métodos desenvolvidos para irem além da oferta de bens e serviços, e visam definir padrões de consumo, de controle, influenciar consciências, retirar a liberdade de escolha do indivíduo e estabelecer padrões discriminatórios, mediante a ameaça e violação dos direitos fundamentais como a privacidade, a igualdade e a liberdade, antes e após a coleta das informações.

Outrossim, há uma carência de ética e justiça no tratamento de dados como meras estatísticas e a utilização da tecnologia contra a própria individualidade dos usuários, dada a existência de máquinas capazes de conhecer melhor o homem do que ele mesmo. O caso do metro de São Paulo é utilizado para explicitar a existência e o *modus operandi* da coleta indiscriminada dessas informações, e comprova a imperiosa necessidade de regulação e fiscalização do tratamento de dados.

Apesar da tutela constitucional e da existência de legislações esparsas sobre o tema, as práticas violadoras permaneceram em ascensão. Foi diante da impossibilidade de uma vida austera em isolamento que surge a LGPD para dar transparência às instituições públicas e privadas em relação aos titulares dos dados. Diferente do que se pensa, a sociedade não serve ao Direito, mas o Direito deve servir a sociedade em suas constantes transformações. Fronteiras são expandidas a cada segundo e, nesse sentido, os desafios jurídicos se reinventam. A lei de proteção de dados traz inovações quanto a práticas corriqueiras que agora são ilegais. A adequação à lei exige pressa, visto que as penalidades são rigorosas.

Também é necessário conceber a ideia de que a LGPD e a ANPD isoladamente não proporcionarão a solução de todos os conflitos envolvendo proteção de dados pessoais, mas a cooperação entre a autoridade e outros órgãos conjuntamente ao diálogo das fontes poderão redirecionar o futuro ético e mercadológico dos setores publico e privado. O Estado também enfrentará desafios para adequação a LGPD, que exigirá maior segurança e rigor quanto a coleta e segurança de informações pessoais. Ademais, o assunto carece de inclusão e debate nas instituições de ensino de Direito.

REFERÊNCIAS

BEZERRA, André Luís Martins. **A Lei 13.709/18 e os novos desafios da proteção de dados pessoais e identidade**. 2019.

BRAGHIT, Ronaldo. **Business Intelligence:** Implementar do jeito certo e a custo zero. São Paulo: Casa Código, 2017.

BLUM, Renato Opice; ELIAS, Paulo Sá. O consumidor do século XXI. **Revista do Advogado.** Ano XXXI. n.114.São Paulo: Associação dos Advogados de São Paulo, dez. 2011.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1348532/SP.** (Quarta Turma). Relator: Ministro Luis Felipe Salomão. Brasília, de 10 de outubro de 2017. Disponível em: https://scon.stj.jus.br/SCON/. Acesso em: 10 jul. 2020.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1168547/RJ.** (Quarta Turma). Relator: Ministro Luis Felipe Salomão. Brasília, de 11 de maio de 2010. Disponível em: https://scon.stj.jus.br/SCON/. Acesso em: 10 jul. 2020.

BRASIL. **Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua, Ano 2017**. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 25 maio 2020.

BRASIL. **Decreto-Lei nº 13.709, de 14 de agosto de 2018**. Regulamenta o tratamento de dados pessoais no Brasil, tanto pelo poder público quanto pela iniciativa privada. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 abr. 2020.

BRASIL. Supremo Tribunal Federal. **Plenário retoma nesta quinta-feira (28) julgamento de ações sobre bloqueio de aplicativos de mensagens**. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=444283. Acessado 5 jun. 2020.

BRASIL. Ministério da Economia. **Economia com implantação de serviços digitais pode gerar economia de 97% aos cofres públicos.** 2017. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/planejamento/economia-com-implantacao-de-servicos-digitais-pode-gerar-economia-de-97-aos-cofres-publicos. Acesso em: 10 jul. 2020.

CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz e Terra, 2002.

COMISSÃO EUROPEIA. **Assuma o controle de seus dados: um guia do cidadão para a proteção de dados na UE.** Luxemburgo: Serviço das Publicações da União Europeia. 2018.

CONESA, F. **Derecho à la intimidad, informática y Estado de Derecho**. Valencia: Universidad, 1984.

DANTAS, Haendel. **Um mosaico de pessoas:** Barack Obama. 2008. Disponível em: https://comunicadores.info/2008/03/26/barack-obama-um-mosaico-de-pessoas/. Acesso em: 30 maio 2020.

DOMINGOS, Pedro. **O Algoritmo Mestre:** Como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. São Paulo: Novatec Editora Edição, 2019.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais.** Rio de Janeiro: Renovar, 2006.

FRAZÃO, Ana. **Plataformas digitais e os desafios para a regulação jurídica**. v.1. Belo Horizonte: Editora D'Plácido, 2018.

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

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Petrópolis: Vozes, 2014.

GNIPPER, Patrícia. **Seu smartphone seria poderoso o suficiente para te levar até a Lua?** 2019. Disponível em: https://canaltech.com.br/espaco/seu-smartphone-seria-poderoso-o-suficiente-para-te-levar-ate-a-lua-144515/. Acesso em: 20 abr. 2020.

GUIMARÃES, Patrícia Borba Vilar. Monetização De Dados Pessoais Na Internet: Competência Regulatória A Partir Do Decreto Nº 8.771/2016. v. 4, nº1. Artigo. **Revista de Estudos Constitucionais UFRN.** 2018.

HARARI, Yuval Noa. **Homo Deus:** uma breve história do amanhã. Disponível em: http://lelivros.love/book/baixar-livro-homo-deus-yuval-noah-harari-em-pdf-epub-e-mobi-ou-ler-online/. Acesso em: 20 maio 2020.

HELTON, Simões Gomes; LAPORTA, Taís. **Entenda o que é blockchain, a tecnologia por trás do bitcoin**. 2018. Disponível em: https://g1.globo.com/economia/noticia/entenda-o-que-e-blockchain-a-tecnologia-por-tras-do-bitcoin.ghtml. Acesso em: 20 abr. 2020.

HOWARD, Dresner; TONI, Ronaldo. **Business Intelligence**: Implementar do jeito certo e a custo zero. São Paulo: Casa Código, 2017.

IBGE. Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua" Ano 2017. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2017.** Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 25 maio 2020.

JOTA. **Sorria? Seus dados estão sendo compartilhados**. 2018. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/sorria-dados-compartilhados-29032018. Acesso em: 20 abr. 2020.

JOTA. **O valor positivo da LGPD.** 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-valor-positivo-da-lgpd-25112019. Acesso em: 10 jul. 2020.

LÈVY, Pierre. **Cybercultura.** Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMBERGER, Têmis. **Proteção de dados Pessoais e comércio eletrônico:** os desafios do século XXI, São Paulo: Vozes, 2008.

MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** Linhas gerais de um novo direito fundamental. São Paulo: Saraiva Educação, 2017.

MIGUEL, Fernando Gomes. **Os desafios do Brasil na nova era da proteção de dados pessoais e da privacidade**. 2019. Disponível em: https://www.migalhas.com.br/depeso/298736/os-desafios-do-brasil-na-nova-era-da-protecao-de-dados-pessoais-e-da-privacidade. Acesso em: 10 jul. 2020.

OLIVEIRA, Eduardo Chagas; CARNEIRO, Ivana Libertadoira Borges. Sobre o caráter persuasivo da estrutura panóptica: Bentham, Foucalt e as novas tecnologias. **Revista Ideação**. n. 33. 2016.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018-LGPD. São Paulo: Saraiva Educação, 2020.

RENASCENÇA. Dados pessoais e dados pessoais sensíveis, 2018. Disponível em: https://rr.sapo.pt/privacidade-online/cap1.aspx. Acesso em: 20 abr. 2020.

RIBEIRO, Jose Antonio. **Big Data para Executivos e Profissionais de Mercado**. Rio de Janeiro: Método, 2018.

RUARO, Regina Linden, RODRIGUEZ, Daniel Piñeiro, FINGER, Brunize. O Direito à Proteção de Dados Pessoais e a privacidade. **Revista da Faculdade de Direito da Universidade Federal do Paraná**. Curitiba. n. 53. 2011.

SARLET, INGO WOLFGANG. **Série Direito Inovação e Tecnologia-Direito, Inovação e Tecnologia:** volume 1. São Paulo: Saraiva Educação, 2017.

SCHAAR, Peter. Das Ende der Privatsphäre: der Weg in die Uberwachungsgesellschaft. Munchen, C. Bertelsmann apud RUARO, Regina Linden. O Direito à Proteção de Dados Pessoais e a Privacidade. 2011. **Revista da Faculdade de Direito UFPR.** Disponível em: https://revistas.ufpr.br/direito/article/view/30768. Acesso em: 20 maio 2020.

SCHWAB, Klaus. **A Quarta Revolução Industrial.** Rio de Janeiro: EDIPRO, 2019.

SOUZA, Maria Luciana Pereira de. **Proteção de dados pessoais na internet:** a mais recente instrumentalização do princípio da dignidade humana na sociedade da informação. Rio de Janeiro: Vozes, 2018.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet.** v. 22. Fortaleza: Pensar, 2017.

VEIGA, Alfredo Neto. **Foucault & a Educação.** São Paulo: Autêntica Editora, 2019.

VELOSO, Thássius. **WhatsApp em números: 120 milhões de brasileiros e 100% de criptografia.** 2017. Disponível em: https://www.techtudo.com.br/noticias/2017/05/whatsapp-em-numeros-120-milhoes-de-brasileiros-e-100-de-criptografia.ghtml. Acesso em: 05 de junho de 2020

VIGNOLI, Richele; VECHIATO, Fernando. **Dados sensíveis no contexto dos dados de pesquisa: um olhar na perspectiva da Ciência da Informação.** 2019. Disponível em: 10.31229/osf.io/dkn8z. Acesso em: 20 abr. 2020.

ZUBOFF, Shoshana. **Um capitalismo de vigilância:** Le Monde Diplomatique. 2019. Disponível em: https://diplomatique.org.br/um-capitalismo-de-vigilancia/. Acesso em: 20 abr. 2020.

WIFI METRO SP. **Termos e Condições. Termos de Privacidade**. 2017. Disponível em: http://freewifimetrosp.com.br/. Acesso em: 20 abr. 2020.

WHATSAPP. **FAQ do WhatsApp - Criptografia de ponta a ponta**. https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption. Acessado 5 jun. 2020

WU, Tim. **The atention merchants: the epic scramble to get inside our heads**. New York: Knopf, 2016.