

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

ICARO UCHÔA DE FREITAS

2020 x 1984: RELAÇÕES ENTRE TECNOLOGIA E PRIVACIDADE
JOÃO PESSOA
2020

ICARO UCHÔA DE FREITAS

1984 x 2020: Ensaio sobre as ameaças à privacidade na obra e na realidade

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

Orientador: Prof. Marcelo Weick Pugliese

JOÃO PESSOA

2020

ICARO UCHÔA DE FREITAS

2020 x 1984: RELAÇÕES ENTRE TECNOLOGIA E PRIVACIDADE

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

Orientadora: Prof. Marcelo Weick Pogliese

**Catalogação na publicação
Seção de Catalogação e Classificação**

F8662 Freitas, Icaro Uchôa de.
2020 x 1984: relações entre tecnologia e privacidade /
Icaro Uchôa de Freitas. - João Pessoa, 2020.
58 f. : il.

Orientação: Marcelo Weick Pugliese.
TCC (Graduação) - UFPB/CCJ.

1. Direito. 2. Tecnologia. 3. Privacidade. 4.
Literatura. I. Pugliese, Marcelo Weick. II. Título.

UFPB/CCJ

CDU 34

DATA DA APROVAÇÃO:

BANCA EXAMINADORA:

Prof. Prof. MARCELO WEICK POGLIESE
(ORIENTADOR)

Prof. FÁBIO FIRMINO DE ARAÚJO
(AVALIADOR)

Prof. FÁBIO BEZERRA DOS SANTOS
(AVALIADOR)

RESUMO

O presente trabalho visa analisar as possíveis ameaças ao direito à privacidade na sociedade atual e relacioná-las com a obra do escritor George Orwell, 1984. Relacionando assim, conceitos como Big Data e Internet das coisas, com a realidade da distopia, e também fazer a comparação do cenário literário com a realidade, sobre quais pontos se tornaram parecidos ou não. Fazendo a ponderação de até onde os instrumentos hoje de controle social e vigilância assemelham-se aos instrumentos usados em Oceania (país onde vive o protagonista da obra). Realizando um importante diálogo entre direito e literatura, duas das artes mais próximas do ser humano. Além de mostrar um pequeno panorama da legislação sobre privacidade hoje no cenário nacional, mostrando alguns dispositivos chave da Lei Geral de Proteção de Dados, aprovada recentemente no Brasil, e quais eram os instrumentos normativos antes dessa aprovação, e quais estão além da referida lei, como a constituição nacional, código civil brasileiro dentre outros.

Palavras-chave: Tecnologia. Privacidade. Literatura.

SUMÁRIO

1 INTRODUÇÃO	9
2 - O USO DOS DADOS NO DIA A DIA	11
2.1 - Histórico e evolução da informação	11
1.2 - Novos meios de produção e coleta de dados(Big Data)	15
1.3 - Internet of Things (IoT)	16
1.4 - Redes Sociais	21
1.5 - Desafios à Privacidade pela Coleta de Dados	23
2 - REGULAÇÃO NO USO DE DADOS	28
2.1- Evolução do direito à privacidade	28
2.2 - Lei Geral de Proteção de Dados (13.709/18)	32
2.2.1 - Legislação Pré LGPD	32
2.2.2 - Normatização da Lei Geral de Proteção de Dados	35
3 - A PRIVACIDADE DOS DADOS SOB A ÓTICA DE “1984”	42
3.1 - Contexto da Obra	42
3.2 A realidade da década 2020 frente às perspectivas traçadas por Orwell	47
5 - CONSIDERAÇÕES FINAIS	52
REFERÊNCIAS	54

Lista de Tabelas

Tabela 1 - Tipos de conectividade do celulares no brasil.....	18
Tabela 2 - Tempo para atingir 50 milhões de usuários.....	20

Lista de Ilustrações

Imagen 1 - Países com legislação sobre privacidade de dados no mundo.....	30
Imagen 2 - Mapa mundi na obra “1984”	42

1 INTRODUÇÃO

O presente trabalho visa analisar as inovações tecnológicas advindas com a revolução digital vivenciada atualmente, em que cada vez se carrega mais de si mesmo no seu bolso e em aparelhos externos. Hoje, conceitos como Internet das Coisas e Big Data começam a ser mais falados todo dia, e mais utilizados também, essa situação reflete o dia a dia em 2020, em que estamos passíveis de ser vigiados por um terceiro a cada momento, relógios inteligentes monitoram nosso sono, celulares verificam nossa voz, nossas pesquisas e mensagens, redes sociais usam nossa interação para nos direcionar conteúdos personalizados etc.

Toda essa situação de inserção no meio digital levou o indivíduo a ter tudo registrado, gravado e arquivado, mas não mais em um pen drive físico, que lhe pertence, mas sim em uma nuvem de terceiros, muitas vezes gratuitas. Ocorre que, como já diz o ditado, “não existe almoço grátis”, sendo assim essas gigantes tecnológicas utilizam dos dados armazenados para personalização de propagandas e vendas destes para terceiros.

A situação descrita leva o questionamento, devido ao quanto difícil é estar separado da internet hoje, de qual o risco dessa nova interação traz ao direito à privacidade, sendo possível analisar como esses métodos de coleta de dados, que em última análise, são bem invasivos, conversam com a privacidade do indivíduo.

E, embora tal situação seja extremamente atual devido ao avanço tecnológico dos últimos 30 anos, ainda assim não é possível afirmar que ele era imprevisível, afinal alguns autores já trataram em obras sobre uma temática semelhante, mas à sua época estavam apenas sugerindo futuros utópicos, ou distópicos, e não a realidade vivida.

Um dos autores que tratou de uma temática similar, no tocante à sociedade de vigilância, foi o inglês George Orwell, que em seu livro “1984” traz a tona uma previsão de uma sociedade futurista, com profundo controle social do indivíduo, da

informação que este consome, e que tenta o vigiar o máximo possível. Até mesmo criando em sua obra uma televisão reversa, a teletela, que nada mais era do um aparelho que passava propaganda todo o dia na casa dos cidadãos, e mais, ainda vigiava o que os mesmos faziam ou diziam.

Dessa forma o presente estudo visa realizar a análise dos possíveis riscos trazidos à privacidade da nova imersão tecnológica vivida, mostrar como essa situação está sendo regulada no Brasil, e fazer o diálogo com a literatura, no presente caso com o livro 1984 de George Orwell.

Para tal foi feito levantamento bibliográfico com diversos autores que tratam da temática da tecnologia e sua interação com o direito, legislação quanto às normas aplicáveis no Brasil, e com a obra do autor inglês.

Visando ao longo do trabalho examinar um pouco essa interação da privacidade com a tecnologia, e relacionar com o pensamento de Orwell em 1949, vendo em que aspectos está parecido, e em quais aspectos até mesmo foi superada a realidade prevista por ele.

2 - O USO DOS DADOS NO DIA A DIA

2.1 - Histórico e evolução da informação

O uso da informação pela sociedade, seja pelos entes governamentais ou pelas entidades privadas, sempre teve um papel e valor de extrema importância, pois como diz o ditado “conhecimento é poder”. Porém quando tratamos de um uso sistematizado dessas informações podemos ver o quanto difícil e ao mesmo tempo, o quanto vantajoso é utilizar tais métodos.

Desde as primeiras formas de acumular conhecimento, como a invenção da escrita, a capacidade de transmitir informações pelo uso de símbolos mutuamente reconhecidos além de garantir que o conhecimento fabricado pelo homem fosse repassada para as novas gerações, também permitiu que estas informações fossem armazenadas.

Ocorre que, antes da organização das sociedades mais próximas de algo conhecido como os estados modernos é difícil falar sobre organização sistemática de informação pela sociedade, até porque o próprio conceito de sociedade está em cheque.

Mas, ainda assim, podemos rastrear onde e de que modo essa prática de acúmulo e uso de informações, especialmente sobre a população, começou a ser usada. Com a formação de sociedades, cidades-estado, impérios, começamos a ter os requisitos necessários para que este agrupamento de informações começasse a ocorrer, entre eles, os recursos financeiros e humanos para realizar tais empreitadas, e interesse e o incentivo para a sua realização.

A sociedade ao longo da história trabalhou com poucos dados não porque o quisesse, mas porque era a única alternativa, como citado por Mayer-Schonberger e Cukier (2013, p. 19) The challenge of processing large piles of data accurately has

been with us for a while. For most of history we worked with only a little data because our tools to collect, organize, store, and analyze it were poor.”

Quanto a questão dos recursos é materializado em razão de que com a existência de estruturas de poder centralizadas, onde há a acumulação de recursos (no caso os reis e representantes desses Estados) há a possibilidade que dezenas, centenas ou até milhares de pessoas trabalhem em função de um fim comum sob a coordenação de uma autoridade central. Mas nas primeiras cidades, há mais de 7.000 mil anos atrás já era possível ver que após as civilizações, o acúmulo de informações vem em seguida, Mayer-Schonberger e Cukier (2013, p. 20)

The oldest record of counting dates is from around 5000 B.C., when Sumerian merchants used small clay beads to denote goods for trade. Counting on a larger scale, however, was the purview of the state. Over millennia, governments have tried to keep track of their people by collecting information.

E esse é um requisito para que a empreitada de coleta de informações acerca de uma população seja realizado, mas como é esperado, as sociedades antigas careciam de diversas matérias para poder dispor de seus recursos em pontos que não fossem urgentes ou necessário, por isso esse ponto não é suficiente para o começo da coleta de informações em massa da população.

E em relação a necessidade de realizar tal empreendimento, que seja, é necessário que haja interesse e ganhos a vir do alocamento dos recursos existentes nessa respectiva tarefa, pois assim essa atividade irá passar na frente das outras concorrentes na visão da autoridade capaz de executá-la.

Assim, podemos vislumbrar um dos primeiros métodos de utilização para a produção e acúmulo de informação em massa sobre os indivíduos de uma sociedade, os census. O censo, do latim “*census*”, que significa, de acordo com Comissão Nacional de Classificação do IBGE (2020) “Pesquisa realizada periodicamente para calcular número de pessoas de um país, de um grupo social etc.;” é utilizado até hoje por nossas sociedades com os mais diversos fins, e remonta a milhares de anos atrás, devido a conseguir cumprir os requisitos já mencionados, era uma tarefa executável, e tinha importância suficiente para ser realizada. Afinal, a atividade embora árdua não é de extrema complexidade, a

depender das informações a serem coletadas poderá ser bem simples até, e no mais, é um ponto necessário à organização estatal, pois assim é possível definir as populações de determinadas regiões, seus bens etc. Informações que serão cruciais para a coleta de impostos, convocação de soldados, concessão de benefícios dentre outros.

Dito isso, podemos ver que o censo, embora de uma forma mais antiga, já pode ser visto como um meio de coletar e organizar informações sobre as pessoas de uma região, como mencionado pela Comissão Nacional de Classificação do IBGE (2020) têm-se registro de censos realizados na região da atual China há mais de 4 mil anos atrás (2238 a.c.). E não apenas lá, tal prática se tornou praxe em todos os lugares onde o sistema político e econômico prosperava, em Roma, por exemplo, como citado por Beardy (2017) houveram 72 censos dentre o primeiro realizado pelo Rei Sérvio Túlio em 555 a.c e 72 d.c. E assim em outras sociedades ao redor do globo, essa e outras formas de coletas de dados foram utilizadas como uma forma de ajudar o desenvolvimento das culturas, além de possibilitar maior controle central de uma autoridade sobre sua população.

Com a evolução da sociedade e a consequente evolução tecnológica os meios de agrupar informações sobre as populações só aumentou, e também os meios de armazenar tais dados. Como exemplo a invenção da prensa por Gutemberg em 1453 possibilitou uma revolução na produção e reprodução de livros, esses que também são instrumentos de acúmulo de informações utilizadas, por exemplo, pelos Estados, possibilitando assim que as informações uma vez obtidas pudesses sem difundidas com maior facilidade.

Da mesma forma a quantidade de informação armazenável também aumentou, de forma que na idade média e pré revolução industrial as sociedades já tivessem um controle muito maior das atividades realizadas pelos indivíduos.

Efeito das novas formas de acompanhar a vida do indivíduo foi o trabalho publicado por Sameul Warren e Louis Brandeis em 1890, o artigo tratava de um

novo direito, direcionado a defender um bem que até então não tinha uma defesa per si, a vida privada do cidadão.

À época de vida destes dois autores, então egressos da faculdade de direito de Havard, já havia a novidade tecnológica das câmeras fotográficas, essa invenção mudou o conceito de mundo, e de vida privada também, afinal, anteriormente a única forma de registrar um ato da realidade era por meio de um desenho, que em muitos casos tinha maior função de retratar o que se queria lembrar do que a realidade em si. Como explicado por Mendes (2017) os autores americanos inovaram ao trazer o conceito de privacidade para o campo do direito à personalidade, rompendo com tradição que colocava a privacidade ligada ao direito à propriedade.

De qualquer forma era impossível ter a confiabilidade em um quadro, pois ele não era uma reprodução da realidade, a foto o era, e dessa forma poderia, diferentemente de um quadro, retratar e registrar diversas situações de forma fidedigna, mesmo sem a vontade dos participantes da foto, por exemplo ao registrar o convívio interno na casa de uma família, só seria possível anteriormente com quadros e autorização dos mesmos.

Além desta, outras invenções mudaram o mundo com sua difusão no século XIX, as cartas já tinham como concorrentes os telégrafos, já era possível realizar ligação por meio de telefone etc.

E se em 1890 dois juristas já tinham clamado pela criação do “*Right to Privacy*” em função da difusão das tecnologias mencionadas, não lhes foi possível notar as tecnologias vindouras com a 4º revolução industrial, a revolução tecnológica computacional, que permitiu conceitos como Internet das Coisas, Smartphones, Notebooks, relógios inteligentes etc.

1.2 - Novos meios de produção e coleta de dados(Big Data)

E este é o cenário mundial em 2020, hoje o mundo como vivido pelos autores do “Right to Privacy” nos pareceria uma sociedade utópica (ou distópica) sobre o quesito da informatização das coisas, e sobretudo na questão relacionada à privacidade.

Hoje, um dia a dia digno dos filmes de ficção científica é totalmente possível, afinal, os últimos 40 anos foram de mudanças inimagináveis para nossos antepassados. Como mencionado por Mendes (2017 posição 200):

“Efetivamente, a doutrina considera que a capacidade de criar, manipular, armazenar, transmitir, compartilhar e unir informação digital é a mais influente inovação do século XX, que representa uma força dominante do século XXI”.

Um cidadão hoje pode acordar ás 6 da manhã e ter todos os seus impulsos e qualidade do sono já monitoradas, usar seu assistente pessoal de voz para perguntar as horas e colocar uma música, se locomover ao trabalho por meio de aplicativos no smartphone, o motorista usará outro aplicativo para saber o caminho com menos trânsito. Chegando ao trabalho ainda terá todas as pesquisas que fez na internet registradas, pedirá o almoço por meio de aplicativo, todos os passos que deu, estimativa de calorias gastas serão quantificadas pelos seus dispositivos.

Irá também se comunicar com seus contatos via aplicativos de mensagens, e mesmo tendo o dia ocupado poderá acompanhar o dia de seus amigos e de pessoas que ele nunca viu em tempo real. A noite chega e ao voltar para casa poderá realizar ligações de vídeo com pessoas em qualquer lugar do mundo, assistir filmes indicados especificamente para ele de acordo com seus hábitos e poderá ler um livro em um e-reader, onde milhares de livros cabem na palma da mão.

O dia desse cidadão está totalmente dependente da interconectividade, desde de acordar até dormir, tudo o que ele fala poderá escutado pelo seu celular, tudo que pesquisa será registrado pelo site de pesquisas, por onde andou será registrado pelo GPS de algum de seus dispositivos, com quem conversou dentre outros pontos.

E todo esse processo de produção de dados tem importância e consequência para o indivíduo que o produz, segundo Magrini (2019)

os dados de uma pessoa possuem, ao mesmo tempo, um caráter existencial que se revela preponderantemente na proteção da privacidade e da identidade da pessoa humana — em decorrência da tutela de sua dignidade —, e um caráter patrimonial, que se identifica pela possibilidade do uso desses dados como insumo para o desenvolvimento de atividades empresariais das mais diversas áreas.

A realidade parece esmagadora frente ao que o indivíduo poderia clamar como “privacidade”, afinal, ele não está mais só um segundo sequer.

Porém como mencionado por Mayer-Schonberger e Cukier (2013, p. 96, tradução nossa) é necessário fazer a ponderação histórica do momento que estamos vivendo, uma verdadeira revolução digital:

We are in the midst of a great infrastructure project that in some ways rivals those of the past, from Roman aqueducts to the Enlightenment's Encyclopédie. We fail to appreciate this because today's project is so new, because we are in the middle of it, and because unlike the water that flows on the aqueducts the product of our labors is intangible. The project is datafication. Like those other infrastructural advances, it will bring about fundamental changes to society.

E nesse modelo os negócios vão ficando cada vez mais aprimorado, como mencionado por Mayer-Schonberger e Cukier (2013), essa foi uma das ideias implementadas na Amazon para aprimorar a venda de livros, utilizar os dados das compras de seus clientes, para assim levantar os seus possíveis gostos e conseguir recomendar novos livros para sua próxima compra. O processo realizado na empresa utilizou uma quantidade imensa de dados, mas acabou por resultar que hoje um terço das compras na Amazon é realizada com base nas recomendações e na personalização do sistema.

Para entendermos tal situação é necessário que compreendamos também alguns pontos que fazem tal situação ocorrer.

1.3 - Internet of Things (IoT)

Um dos conceitos necessário para o entendimento da nova realidade humana é o da Internet das Coisas (*Internet of Things*), que retrata a nova relação entre homem máquina não só em situações ou serviços, mas em quase todas as tarefas de um indivíduo no seu dia. Como definido pelo Magrini (2018):

“A internet das coisas, à parte maiores rigores semânticos, é um termo que acaba evocando o aumento da comunicação entre máquinas pela internet (M2M, ou machine-to-machine, que recentemente ultrapassou em volume a comunicação interpessoal pela internet),

Dessa forma pode-se ver que a IoT tem esse aspecto de ser a comunicação entre máquinas (M2M), e esse conceito de máquinas capaz de realizar comunicação entre si é expandido, já que cada vez mais objetos do cotidiano são passíveis de se tornarem inteligentes.

Tênis com sensores que medem passos, relógios que monitora batimentos cardíacos, lâmpadas com acionamento via smartphone, assistentes de voz para casa dentre outros, são alguns dos exemplos de objetos inteligentes, em maior ou menor medida.

Assim, há uma mudança na atuação das pessoas frente aos seus objetos, pois ela começa a ser também uma produtora de material e dados de forma constante. Afinal a substituição do manual pelo tecnológico tem consequências inerentes a tal, Silvera (2017):

Uma fechadura digital aberta por um cartão magnético ou por biometria não somente destrava a porta como também registra o horário exato em que isso aconteceu. Também pode registrar qual cartão magnético ou digital abriu a porta, no caso de existir mais que um. A parte física do dispositivo é comandada por sua parte lógica gerando um conjunto de informações que ficam armazenadas em um software. As tecnologias digitais produzem um conjunto de informações todas as vezes que são utilizadas.

Outro fator a ser considerado é que já que todo esse procedimento de uso de objetos ligados a internet e comunicando-se entre si é uma nova realidade, os seus limites ainda tenderão a ser encontrados.

Tanto pela sua real utilidade no dia a dia, que poderá ser questionada em alguns casos, como exemplo o dispositivo egg minder (CARDOSO, 2013), que nada

mais é do que uma bandeja de ovos digital, que enviará mensagem para seu smartphone quando os ovos acabarem.

Tanto pelo aspecto da real invasão de privacidade que há com esses objetos, e dos riscos inerentes a ter todo o seu ambiente conectado, como exemplo há a situação da boneca Cayla, que, como demonstrado pela matéria da BBC (2020) , é um brinquedo inteligente, podendo responder perguntas e interagir com as crianças, ocorre que ela também tinha uma câmera e mais, houveram problemas com sua segurança e possibilidade de hackers invadirem seu sistema, gerando com que a agência de telecomunicações da Alemanha soltasse uma recomendação para destruição de Cayla, pelo risco de invasão aos dados pessoais.

E também pelo principal fator da utilização da coleta de dados, que é gerar uma personalização do produto, por exemplo, como citado por Mayer-Schonberger e Cukier (2013, p. 89)

It is not just people but objects that can be tracked now. With wireless modules placed inside vehicles, the datafication of location will transform the idea of insurance. The data offers a granular look at the times, locations, and distances of actual driving to better price risk. In the U.S. and Britain, drivers can buy car insurance priced according to where and when they actually drive, not just pay an annual rate based on their age, sex, and past record.

Ainda assim o ponto de equilíbrio ainda será encontrado, já que hoje ainda está sendo verificado o pleno crescimento dos dispositivos inteligentes em número e em funcionalidades.

As estimativas variam, mas espera-se que em 2020 hajam entre 30 (MARTINEZ, 2016) a 50 bilhões (NORDRUM, 2016) de dispositivos conectados à internet, o que dá cerca de 4 a 7 dispositivos por pessoa, ou muito mais, se considerarmos o número de pessoas que realmente usam a internet em seu dia a dia, estimado em cerca de 2 bilhões.

In 2003, there were approximately 6.3 billion people living on the planet and 500 million devices connected to the Internet.³ By dividing the number of connected devices by the world population, we find that there was less than one (0.08) device for every person. Based on Cisco IBSG's definition, IoT didn't yet exist in 2003 because the number of connected things was relatively small given that ubiquitous devices such as smartphones were just being introduced. For example, Steve Jobs, Apple's CEO, didn't unveil the iPhone until January 9, 2007 at the Macworld conference.

Explosive growth of smartphones and tablet PCs brought the number of devices connected to the Internet to 12.5 billion in 2010, while the world's human population increased to 6.8 billion, making the number of connected devices per person more than 1 (1.84 to be exact) for the first time in history.⁵

Dessa forma é clara a realidade da nova sociedade digital em que estamos cada vez mais inseridos, e dentre todos os dispositivos que participam de nosso dia a dia e coletam dados, podemos citar o mais influente de longe, os Smartphones.

A evolução dos Smartphones se deu ao longo da segunda metade dos anos 2000, embora sua explosão ocorra com a virada para a segunda década do milênio, em que os celulares tiveram uma difusão completa na sociedade, e cada vez mais baseada em smartphones.

Os dados (TELECO, 2020) indicam que em setembro de 2020 havia mais celulares que pessoas no Brasil, cerca de 228 milhões de celulares, enquanto a população está estimada em 212 milhões (IBGE, 2020). Deste, é possível verificar o nível de conectividade de acordo com a tecnologia de conexão utilizada, vejamos:

Tabela 1 - Tipos de conectividade do celulares no Brasil

2G	3G	4G
27.714.452	35.139.977	165.441.991
12,1%	16,2%	72,4%

Logo, podemos notar também que em sua grande maioria os celulares hoje são smartphones, podendo se verificar tal questão por mais de 70% dos celulares terem conexão 4G, e ressaltando que a conexão 3G, embora não seja a mais atual, em grande parte já é uma conexão para smartphones, logo, o número de Smartphones no Brasil está próximo de 90% do total de celulares.

Em termos globais, dados da União Internacional de Telecomunicações (UTI) mostram que em 2018 cerca de 95% das pessoas já vivem em área com acesso a rede 2G ou superior, 84% tem acesso à banda larga móvel, e a 4G já estava acessível a cerca de 4 bilhões de pessoas.

Parte desse fenômeno é verificado em razão da evolução do conceito de celular, embora nos primórdios de sua massificação tivesse uma função praticamente de apenas ligar, não só porque era o oferecido, mas também pois era o procurado em um celular.

Porém com a difusão dos celulares inteligentes, estes começaram a demonstrar uma clara evolução em suas funcionalidades, e dessa forma seu segmento passou de um telefone residencial portátil, para um conceito de computador de bolso.

Como já mencionado *en passant*, hoje os smartphones suprem muito mais do que apenas a função de ligar, em muitos casos sequer essa função é utilizada, mas ele serve como um aparelho multifuncional, nele pode-se ter um relógio, GPS, calculadora, telefone, televisão, rádio, cartão de crédito, câmera fotográfica, computador para acessar e-mails e, acessar redes sociais, e executar tarefas etc.

Dessa forma, esse aparelho começa a não só acompanhar as pessoas no dia a dia, mas a tomar a atenção destas, já que ele é capaz de focalizar diversas atividades na palma da mão. E por isso mesmo ele é extremamente eficaz em ser um registro e coletar dados de tudo que é feito nele (o que em grande parte já reflete o dia a dia externo ao celular, pois quase tudo está conectado a ele).

Assim essa pequena estação de trabalho consegue registrar não só com quem falamos em ligações, mas sim que páginas acessamos na web, que aplicativos usamos, qual nosso itinerário diário, músicas que ouvimos, cartões que são usados, mensagens enviadas e recebidas, até mesmo o que é falado fora dele, já que os assistentes no geral ficam ligados 24 horas à espera de um comando, e assim sendo capazes de captar o que é falado fora do telefone.

Sobre essa capacidade de captação de áudio passiva é possível rememorar o ano de 2015, onde a como informado por Rusthton (2015)Samsung foi alvo de manchetes em todo o mundo em função de uma função de sempre ouvir o que está sendo dito próximo de seus captadores de som, outro exemplo até então inusitado, foi o pedido para a utilização das gravações da assistente de voz Alexa com fins de

auxiliar em ouvir o que havia se passado em uma residência onde houve um homicídio (BURKE, 2019).

Hoje muito se debate sobre a utilização dessa funcionalidade pelos smartphones também, já que quase todos já contam com algum sistema operacional, mas independente desse fator, é clara a influência que o celular tem sobre o indivíduo, e o quanto deste está naquele, seja em suas agendas, suas conversas, ligações, vídeos, fotos etc.

1.4 - Redes Sociais

E após haver a revisão de alguns aparelhos que têm uso para a coleta de dados, cabe a menção, por último mas não menos importante de alguns mecanismos não físicos que participam desse processo de coleta diária.

Interessante notar que as redes sociais tem uma dimensão jamais imaginada antes, hoje é possível à empresas como o Facebook contar com centenas de milhões, ou até mais de 1 bilhão de inscritos, ou seja, um número de pessoas impensável para poucas gerações atrás, lembrando que a própria evolução populacional é surpreendente no século XX e XXI. A população mundial desde a formação do Homens Sapiens há mais de 100.000 anos atrás levou até o ano de 1800 para ter 1 bilhão de indivíduos vivos, mas em 2010 já atingiu a marca de 7 bilhões de pessoas (FREITAS, 2020).

Então, somando os fatores de grande aumento populacional, com o avanço e disponibilização para grande parte da população do acesso à tecnologia, chegamos a dados surpreendentes. Como demonstrado por Maldonado (2019), segue abaixo o tempo que cada produto levou para ter 50 milhões de usuários:

Tabela 2 - Tempo para atingir 50 milhões de usuários

Automóvel	Celular	Internet	Facebook	Twitter	Pokemon GO
62 anos	12 anos	7 anos	3 anos	2 anos	19 dias

Ou seja, hoje os produtos e serviços digitais crescem muito mais rápido, e vão até número muito maiores que em outros tempos. E esse montante gigantesco de pessoas utilizando diversos desses serviços simultaneamente gera uma quantidade de informações única na história. E todos esses dados não são desperdiçados, afinal diferente de carros ou celulares, os serviços digitais muitas vezes são gratuitos, embora seja extremamente oneroso criar e manter uma plataforma dessa magnitude.

Como citado pelo professor Eduardo Magrini (2018) um estudo da Telefonica estimou que a que a capacidade de processamento de dados em 2020 será na casa dos 800 exabytes (1 exabyte equivale a 1 bilhão de gigabytes), e a maior parte desses dados será enquadrado como dados pessoais, a comparação trazida pelo estudo mostra que em 2015 essa capacidade era de “apenas” 80 exabytes, ou seja, em 5 anos um aumento de 10 vezes.

E grande parte desse volume irá advir do uso das redes sociais, pois com o seu advento, a própria relação do humano com o digital foi alterada, como explicado por Magrini (2018):

Portanto, com o advento da web colaborativa (2.0), o usuário de internet deixou de ser somente um consumidor de conteúdo, passando a ser, ao mesmo tempo, também produtor, dando origem ao conceito de prosumer, típico das relações de interação nas plataformas de web 2.0, principalmente redes sociais.”

Ficando assim latente o alerta sobre como todo esse material é ou será utilizado, afinal, as redes sociais tem um caráter mais íntimo até, afinal, nele postamos imagens pessoais, falamos com amigos, compartilhamos momentos familiares, nesse contexto é mais fácil ao usuário visualizar a importância do sigilo de suas informações.

E embora o uso das redes sociais tenha esse aspecto mais “casual”, também elas serão alvo da dataficação, como mencionado por Mayer-Schonberger e Cukier (2013, p. 91) *Social networking platforms don't simply offer us a way to find and stay in touch with friends and colleagues, they take intangible elements of our everyday*

life and transform them into data that can be used to do new things. Transformando então a interação entre amigos/família/colegas de trabalho etc em dados.

Logo, toda essa estrutura de uma sociedade de vigilância vem a gerar uma série de questionamentos sobre a real efetividade do direito à privacidade em 2020, e as suas perspectivas em um cenário de mudanças tão repentinhas no campo tecnológico.

1.5 - Desafios à Privacidade pela Coleta de Dados

Dessa forma, em parte, há a visão de que a privacidade nada mais é do que uma ficção jurídica, e o direito de ser deixado sozinho é algum conceito ultrapassado, já que a realidade parece vir à contramão e esmagando visão de Warren e Brandeis (2010, p. 4) de que “the right to be let alone, is the most comprehensible of the rights”.

E não surpreende tal visão, pois o cenário pinta um quadro extremamente desfavorável à liberdade de ser deixado só, a tecnologia tomou o século XXI de forma avassaladora, porém ainda cabe o questionamento se há possibilidade de privacidade nesse novo contexto.

Em 404 a.c Atenas realizou um cerco à ilha de Melos, sabedor da incrível superioridade ateniense o general Tucídides fez um ultimato para a rendição dos habitantes da ilha e profetizou “ os fortes fazem o que podem e os fracos sofrem o que devem” (tradução livre), no atual cenário seria então o indivíduo refém de algo mais forte que ele, e ao fraco (o indivíduo) caberia apenas o papel de se resignar e aceitar a derrota de sua vida privada?

Para tentar avaliar tal questionamento primeiro caberá analisar as duas faces das tecnologias e técnicas de processamento já mencionadas. Enquanto Warren e Brandeis (1890) mencionaram o receio de que a fofoca tinha se tornado um negócio, e de as máquinas fotográficas seriam uma invasão à privacidade, hoje esse negócio com o uso de dados pessoais, e os níveis de invasão de privacidade ultrapassaram outras fronteiras não imagináveis então.

Somente o uso dos objetos classificados como “inteligentes”, a chamada internet das coisas, é, segundo Magrini (2018), estimada em ter um impacto global na casa dos 11 trilhões de dólares em 2025, tendo mais de 100 bilhões de objetos até lá, para efeito de comparação, como demonstrado pelo Banco Mundial (2020) esse valor equivale a mais de 6 vezes o PIB do Brasil em 2018, que foi de 1,8 trilhão de dólares.

Complementando, algumas das maiores empresas do mundo hoje são empresas do ramo da tecnologia, como Facebook, Google, Apple, Amazon etc. Ora, ainda assim há uma difusão ao pensar que o Facebook ou o Google estão entre as maiores empresas do mundo mas a grande maioria de seus serviços pode ser usado “gratuitamente”, é aí que entra o valor dos dados.

Um caso interessante mencionado para entender o real impacto que os dados têm nessas empresas ocorreu quando o Facebook lançou suas ações na Bolsa de Valores, enquanto o seu valor segundo os padrões estabelecidos, baseada na estrutura física era avaliado em 6,3 bilhões de dólares, no lançamento a empresa foi avaliada em 104 bilhões, quase 100 bilhões de diferença, como explicado por Mayer-Schonberger e Cukier (2013, p. 119):

How to explain the vast divergence between Facebook’s worth under accounting standards (\$6.3 billion) and what the market initially valued it at (\$104 billion)? There is no good way to do so. Rather, there is widespread agreement that the current method of determining corporate worth, by looking at a company’s “book value” (that is, mostly, the worth of its cash and physical assets), no longer adequately reflects the true value. In fact, the gap between book value and “market value”—what the company would fetch on the stock market or if it were bought outright—has been growing for decades. The U.S. Senate even held hearings in the year 2000 about modernizing the financial reporting rules, which emerged in the 1930s when information-based businesses scarcely existed. The issue affects more than just a company’s balance sheet: the inability to properly value corporate worth arguably produces business risk and market volatility.

E esses dados estão inseridos no contexto de conectividade vivenciado hoje pela sociedade, tendo consequências em diversos campos, por exemplo, se antes havia uma dificuldade em tentar transmitir conhecimento para a posterioridade, hoje há uma dificuldade em até mesmo apagá-lo, ainda mais quando se trata da vida privada das pessoas, como mencionado por Maldonado (2017):

"conquanto o Direito ao Esquecimento possa revelar-se por inúmeras faces diferentes, é efetivamente no ambiente da internet que se concentra a principal problemática acerca do tema, de modo a dar margem a discussões com notável vigor em todo o mundo."

Cabe mencionar também, que por outro lado, a decretação de morte da privacidade é um processo cíclico na sociedade, já tendo a privacidade andado no barco de Caronte, de acordo com as previsões, quando da invenção do telefone, afinal nesse momento as empresas ou telefonistas poderiam ouvir as conversas, quando da invenção do computador, pelo seu poder de processar dados recebidos, com a máquina fotográfica, como mencionado por Warren e Brandeis, da difusão do celular portátil, do computador portátil, e agora, da difusão dos smartphones, tablets, redes sociais etc.

Ocorre que, nessa pretensa, ou real, sociedade de vigilância que está posta, cada vez mais é passível ao indivíduo deixar-se ir, e aceitar que todo o seu trabalho, estudo, pesquisa, mensagens, fotos etc, estarão sujeitos a um terceiro, quando ele os usa ou os acessa via internet.

A preocupaçãoposta parte da realidade de que tal domínio de um ente sobre outro nunca foi possível ao longo da história, afinal nem mesmo o mais poderoso dos reis, um dia pode ter acesso a localização 24 horas por dia de milhões de pessoas, não importasse o quanto quisessem, Genghis Khan, Napoleão, Júlio César e outros jamais poderiam saber o que as pessoas ao seu redor pensam ou querem, mas hoje há acesso e registro de toda pesquisa feita junto à internet.

Existem alternativas para tentar fugir desse controle, ou melhor, dessa vigilância contínua, mas as mesmas são utilizadas apenas por uma porcentagem mínima da população que tem conhecimento técnico para baixar softwares que mudam o IP do computador ou algo do gênero.

Sendo assim, a realidade que se vislumbra é de uma sociedade passível de vigilância por entes externos, tanto o governo, rememorando sonhos de sociedades totalitárias ao longo do século XX, ou de empresas privadas, visto que são elas que fornecem os serviços e coletam os dados diariamente.

O real poder dessas *bigtechs* é algo que ainda está sendo descoberto, e em situações que em muitos casos passam despercebidas, por já serem rotineiras, um exemplo é de quando se faz a pesquisa de um determinado produto, e nos dias seguintes aparecem muito mais anúncios daquele mesmo tipo de produto, ou produtos relacionados.

O que pode parecer inofensivo para alguns pode vir a demonstrar um problema para outros, por exemplo o caso mencionado por Alcantara (2017) em que uma empresa, de acordo os dados de pesquisa de uma moça nos Estados Unidos e usando a sua base de big data e inteligência artificial, descobriu que a moça estava grávida e mandou presentes para ela, visando uma futura cliente, ocorre que, a família não sabia da gravidez, nem mesmo a própria moça, tudo foi com base na aprimorada inteligência artificial que identificou com base na pesquisa dela sobre sintomas relacionados à gravidez. E esse não é um caso isolado no mundo do big data, como citado por Alcantara (2017):

“O que a empresa Target fez é utilizado por várias outras empresas, sempre no intuito de melhorar algo em seu próprio mercado. Contudo, é válido lembrar que nem toda empresa é transparente quanto aos dados coletados ou a sua permissão.

Ou seja, em muitos casos a captura e compartilhamento de dados não é apenas um plus no negócio da empresa, mas o negócio principal, dessa forma ela irá utilizá-los ao máximo.

Mayer-Schonberger e Cukier (2013, p. 125) explicam que existem três principais formas de empresas trabalharem com o big data:

Three types of big-data companies have cropped up, which can be differentiated by the value they offer. Think of it as the data, the skills, and the ideas. First is the data. These are the companies that have the data or at the least have access to it. But perhaps that is not what they are in the business for. Or, they don't necessarily have the right skills to extract its value or to generate creative ideas about what is worth unleashing. The best example is Twitter,

[...]

Second are skills. They are often the consultancies, technology vendors, and analytics providers who have special expertise and do the work, but probably do not have the data themselves nor the ingenuity to come up with the most innovative uses for it. In the case of Walmart and Pop-Tarts, for example, the

retailer turned to the specialists at Teradata, a data-analytics firm, to help tease out the insights.

[...]

Third is the big-data mindset. For certain firms, the data and the know-how are not the main reasons for their success. What sets them apart is that their founders and employees have unique ideas about ways to tap data to unlock new forms of value. An example is Pete Warden, the geeky co-founder of Jetpac, which makes travel recommendations based on the photos users upload to the site.

Após essa explicação, fica mais claro o entendimento do aperfeiçoamento de tal produto (os dados), pois nem sempre a empresa que coleta é que vai utilizar aqueles para ter informações úteis para seu negócio, como explicado por Mendes(2017)

Assim, ao lado das empresas que coletam dados dos seus clientes em razão da necessidade dos serviços oferecidos, surgem também empresas cuja única finalidade é a coleta e o armazenamento da maior quantidade possível de dados pessoais para a sua comercialização e cessão. ChoicePoint, Acxiom e LexisNexis são três das maiores empresas, nos EUA, cuja única finalidade é a comercialização de dados.

Sendo assim, há uma ramificação grande do setor, com cada empresa podendo ser específica em algum de galhos, como a coleta dos dados, o seu processamento, e a sua venda.

E, um fator relevante ao se falar dessa utilização massiva de dados é a normalidade com que está é feita, afinal o uso das redes sociais ou de sites de busca já está aí há alguns anos e aparentemente sem consequências catastróficas para a população, como definiu La Boetie um dos fatores que levam a servidão do cidadão é a habitualidade, ou seja, estar acostumado a determinado fato, e embora o fato da digitalização de nossa sociedade seja recente, ele é muito forte na sua atuação. Dessa forma, como demonstra dados do Comite Gestor da Internet no Brasil (MOVIMENTO, 2018) embora grande parte da população só tenha tido um smartphone ou notebook nos últimos 12 anos, em média um brasileiro fica mais de 9 horas conectado à internet.

Para tentar enfrentar esse possível inimigo invisível, ao longo do século XX e cada vez mais forte no século XXI há um movimento para a implementação de

regras para realizar o controle dos limites em que a coleta de dados poderá ser feita e usada.

2 - REGULAÇÃO NO USO DE DADOS

2.1- Evolução do direito à privacidade

Considerando a evolução tecnológica já mencionada, a situação para o direito também veio a ser construída ao longo do século XX, com uma maior percepção da demanda social no século XXI.

Sendo necessário para os países, muitos deles em formação ou após diversas reconstruções e mudanças de formas de estado, se adequar no tocante a quais regulações as novas tecnologias iriam necessitar, afinal, todo o avanço feito ao longo dos últimos anos criou situações não possíveis anteriormente, e portanto, não reguláveis.

Uma das facetas dessas novas demandas foi justamente a questão relacionada aos dados pessoais da população, até que limite ou não a coleta seria permitida, sob que bases, quem poderia coletar, para o que poderia ser usado etc.

A busca então por essa regulação partia tanto visando controlar e limitar os que seriam coletados pelas empresas, tanto frente aos dados coletados pelos governos, afinal ambos tem uma forte presença e poder sobre as pessoas.

E toda essa inovação veio de forma concomitante com as questões novas que começavam a surgir, dessa forma as respostas encontradas em um primeiro momento não puderam ser definitivas, pois a sociedade evoluiu de forma mais rápida que a legislação em todo o mundo.

Mesmo assim no pós guerra começam a se notar as necessidades envolvidas nesse âmbito, tanto pela recente da utilização de dados de cidadãos para gerar a sua perseguição, como mencionado por Mayer-Schonberger e Cukier (2013, p. 151):

The history of the twentieth century is blood-soaked with situations in which data abetted ugly ends. In 1943 the U.S. Census Bureau handed over block addresses (but not street names and numbers, to maintain the fiction of protecting privacy) of Japanese-Americans to facilitate their internment. The Netherlands' famously comprehensive civil records were used by the invading Nazis to round up Jews. The five-digit numbers tattooed into the forearms of Nazi concentration-camp prisoners initially corresponded to IBM Hollerith punch-card numbers; data processing facilitated murder on an industrial scale.

Mas também no tocante às empresas privadas, afinal o modelo de sociedade de consumo no pós guerra gerou uma nova competição entre as empresas pelo cliente, e como o custo para adquirir clientes era superior ao custo de mantê-los, as empresas então começaram a investir na personalização dos serviços pela utilização de dados dos mesmos, como citado por Mendes (2017):

Nesse sentido, observa-se que existe uma convergência entre a sociedade da informação e a sociedade contemporânea de consumo, na medida em que a economia passa a exigir, para o seu complexo funcionamento, uma quantidade enorme de dados pessoais, possíveis de serem armazenados, processados e transmitidos por meio da tecnologia da informação.

Complementarmente a isso, o direito à inviolabilidade da vida privada estava presente até mesmo na Declaração Internacional de Direito Humanos de 1949, em seu artigo 12º:

Artigo 12

Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Partindo desses pontos, é possível fazer um apanhado das gerações das proteções de dados, e das inovações que elas trouxeram.

No tocando a primeira geração de regulações, é importante frisar o que ela visava limitar, qual era o “inimigo” que a lei foi feita para combater, pois, obviamente não era previsível a situação de 2020 em 1970. Como citado por Mendes(2017):

as leis pretendiam regular os dados que seriam utilizados e processados pelos gigantescos computadores, com grande poder tecnológico à época, enfrentando também a previsão e começo de realidade, da criação de grandes bancos de dados sobre a população.

Como também demonstrado por Mendes (2017) na primeira leva de legislações surgiram por exemplo:

São exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o Fair Credit Reporting Act (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o Privacy Act (1974), aplicável à administração pública.

Na segunda geração ao fim da década de 70 é fortificada a ideia da privacidade e proteção de dados como uma liberdade negativa do indivíduo, e começa a trazer o ideal da criação de instrumentos para a proteção do mesmo. Ideia do consentimento, sendo esse o pilar que deveria gerir as informações pessoais dos cidadãos.

A terceira geração vem também da influência alemã, o pioneirismo da legislação em Hesse ajudou no desenvolver do debate na Alemanha, culminando com uma decisão da suprema corte alemã em 1983 sobre a lei recenseamento de 1982, contribuindo formulação do direito à autodeterminação da informação por parte do usuário.

Que seja, para um entre privado ou público coletar, processar, repassar dentre outras atividades dados de um indivíduo deveria então ser necessário o seu consentimento para tal, o que em última análise é o empoderamento do indivíduo e de se direito.

Na quarta geração, que começa nos anos 90 há a especificação das legislações, dessa forma são desenvolvidas as leis nacionais de proteção de dados, também são criadas as agências de proteção de dados nacionais e são trabalhados instrumentos para o aperfeiçoamento da proteção coletiva.

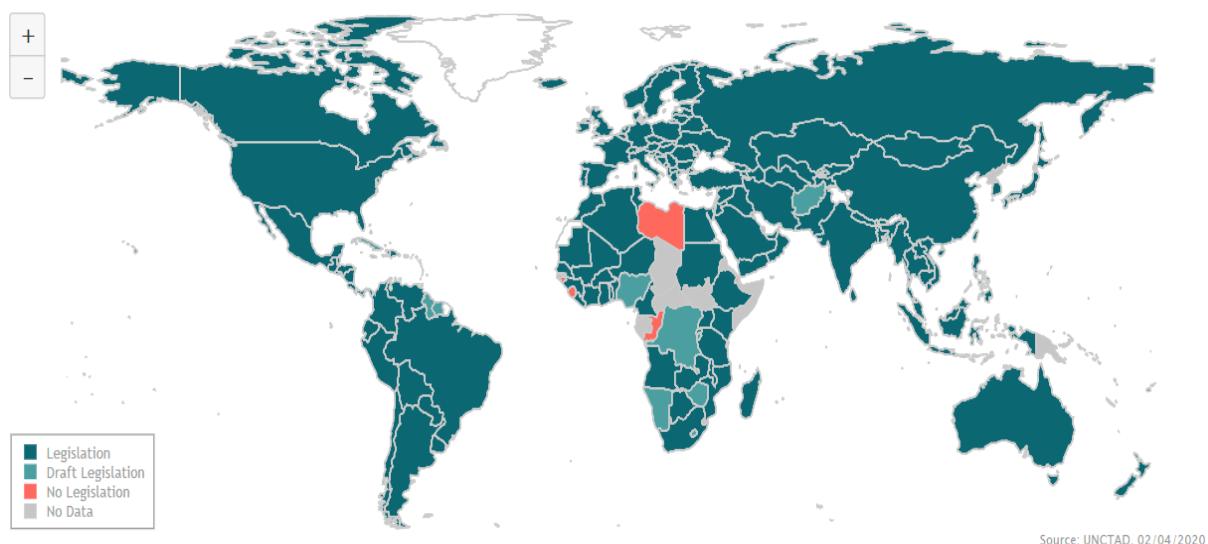
Ao longo dos anos ficou clara a evolução, que começou com as legislações para controle de uma ferramenta nova(os computadores com alto poder de processamento), para a capilarização da defesa do direito à proteção de dados e da privacidade em todas suas formas, como comparação Mendes (2017) cita que:

É de notar que a primeira lei de proteção de dados pessoais do mundo, a Lei do Estado alemão de Hesse, de 1970, limitava-se a regulamentar o

tratamento automatizado dos dados pessoais. Já a Diretiva Europeia 95/46/CE é bastante clara ao tratar ambos de forma indistinta, nos termos de seu art. 3º, 1º: “A presente directiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados”.

Essa evolução veio a criar o movimento pela disseminação da proteção de dados no mundo, em 2020, cerca de 134 países dos 193 presentes na ONU já tinham uma legislação para privacidade e proteção de dados, como mostrado na imagem abaixo, em que os países em verde escuro são os com previsão legal sobre o tema, os em verde claro com projeto de lei, os em laranja sem legislação ou projeto, e os em cinza sem dados sobre.

Imagen 1 - Países com legislação sobre privacidade de dados no mundo



Dessa forma e considerando a especificidade do Brasil, vê-se que o mesmo aprovou a sua lei de proteção de dados e privacidade, a LGPD(Lei Geral de Proteção de Dados) lei 13.709/2018, embora já houvesse um resquício de proteção de dados nas outras normas legais nacionais.

2.2 - Lei Geral de Proteção de Dados (13.709/18)

A lei de proteção de dados brasileira veio não somente pela necessidade real de haver um maior controle e proteção do tema por parte do Estado em defesa do indivíduo, mas também no contexto do Brasil inserido nas novas demandas globais e até mesmo em nível comercial, vejamos Pinheiro (2020):

O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Quanto ao fator econômico, podemos ver a importância da atividade realizada na europa com GDPR (General Data Protection Regulation) 2016/679, pois a invenção do mesmo gerou um fator alavancador em outros países, levando em questão também, como já mencionado, o fator econômico, como citado por Pinheiro (2020) ao se referir a inovação da GDPR:

“Este, por sua vez, ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR.”

A situação também se mostrava necessária devido às consequências ao mundo que esse novo meio de poder e controle das pessoas estava tendo, como explicado por Maciel (2019), o caso da Cambridge Analytica veio a demonstrar os possíveis danos que poderiam ser causados, pois nesse caso, a manipulação de dados ocorrida foi acusada de ter influenciado na eleição americana de 2016, e até no processo de saída do Reino Unido da União Europeia.

No entanto é de se notar que que o Brasil não estava totalmente descoberto acerca de uma legislação de dados antes da LGPD, de fato, a proteção desse objeto já tinha lugar nas legislações brasileiras, em várias leis esparsas.

2.2.1 - Legislação Pré LGPD

Assim, a defesa do direito à privacidade não necessariamente adveio com a LGPD, como mencionado, a própria Declaração Internacional de Direitos Humanos tem uma previsão para este direito (artigo 12). Assim como a legislação pátria também elaborou instrumentos para cuidar da privacidade do cidadão, até mesmo a constituição de 1988 já tinha tal previsão, como está expresso no artigo 5º, X “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;” . O artigo 5º X em combinação com o inciso LXII geram a roupagem de direito fundamental para a proteção de dados, como explicado por Mendes (2017):

“o direito fundamental à inviolabilidade da intimidade e da vida privada, previsto no art. 5º, X, da CF/1988, protege a esfera privada do indivíduo em diversas dimensões, inclusive na dimensão da privacidade dos seus dados pessoais e da autodeterminação de suas informações”; já “a garantia constitucional do habeas data estabelece um direito material à proteção de dados, consubstanciado no direito ao conhecimento, correção e complementação dos dados do titular”, e conclui que “uma interpretação conjunta dos incs. X e LXXII do art. 5º da CF/1988 permite, portanto, falar-se em um direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro”.

A evolução e dispersão dos mecanismos de defesa foram uma característica marcante no ordenamento brasileiro, vejamos, o Código de Defesa do Consumidor, lei 8.078/90 na sua seção VI criou uma regulamentação acerca “Dos Bancos de Dados e Cadastros de Consumidores”:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o

arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

[...]

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Como visto, grande parte das possíveis ocorrências com os dados do consumidor, desde do aviso ao consumidor da sua ficha de cadastro, à correção por erros, já estavam previstas. Outro ponto importante é sobre a necessidade do acesso do consumidor aos dados caso requisitado, e do poder de requisitar sua correção quando houvesse alguma incongruência.

Mas as disposições continuaram a ser mais inovadoras e específicas ao longo dos anos, como mencionado por Marciel (2019) a formulação da Lei 9.296/96, a lei de Interceptação Telefônica e Telemática reconheceu o direito à privacidade e restringindo o uso das interceptações às hipóteses nela previstas, e a lei 9.507/97, a lei do Habeas Datas, garantiu o direito de acesso ao dado do cidadão mesmo quando em poder estatal.

Outro reflexo dessa evolução foi a disposição do Código Civil de 2002, lei 10.406/2002, que trouxe um capítulo sobre os direitos à personalidade, como explicitado nos artigos 20 e 21:

art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.

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

Nos anos dessa década a evolução não cessa, tendo a promulgação de algumas normas como a Lei de Cadastro Positivo, lei nº 12.419/11, a Lei Carolina Dieckmann, lei nº12.737/12, e a Lei de Acesso à Informação, lei nº 12.527/11.

E em 2013 houve a instituição de um novo marco acerca da privacidade na internet no Brasil, o Marco Civil da Internet, como explicado Maciel (2019):

Foi com o Marco Civil da Internet que o Brasil passou a constar em seu sistema jurídico a palavra “privacidade”. Embora curioso, esse fato nada inova, já que “vida privada”, no frigir dos ovos, possui o mesmo sentido. Com o MCI entrando em vigor em 2014, a internet no Brasil passou a ser melhor disciplinada,

Assim a lei do Marco civil trouxe diversas inovações no tocante a legislação da privacidade digital, normatizando o princípio da proteção à privacidade em seu artigo 3º e trazendo outro direitos também ao usuário, como explicado por Maciel (2019):

(art. 7º): VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;^[9] O MCI estabeleceu, na Seção II do Capítulo III, regramento para guarda e disponibilização dos dados pessoais, demandando ordem judicial para acesso ao conteúdo e ainda trouxe os princípios da finalidade e adequação, vedando a guarda, por provedores de aplicações, dos “registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente” e “dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular” (art. 16).

Após a instituição do Marco Civil da Internet e considerando os outros instrumentos já presentes no ordenamento jurídico brasileiro, somado ao contexto já mencionado de evolução da legislação europeia juntamente com os vazamentos de dados cada vez mais comuns, foi se formado o cenário de aprovação da lei de proteção de dados do brasil.

2.2.2 - Normatização da Lei Geral de Proteção de Dados

A lei 13.709/18, a LGPD, vem então como um novo mecanismo, mais amplo e que irá ditar a nova política de tratamento de dados do país, sendo assim, ela vem trazer a nova normalidade e os padrões de segurança e direitos dos usuários.

Dessa forma é pertinente a explicação acerca dos aspectos de maior influência da lei. O primeiro ponto a atentar são as principais definições presentes no artigo 5º da lei:

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;

[....]

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Nestas definições é importante ressaltar a diferenciação entre os “dados pessoais”, e “dados sensíveis”, pois enquanto a lei define o primeiro apenas como uma informação acerca de outrem, o conceito de dado sensível, como explicado por Maciel (2019) já tem um papel mais importante, afinal ele vem a definir o tipo de dado que terá um tratamento diferenciado, afinal, o que o compõe, opção religiosa, orientação sexo, etnia etc, é passível de vir a ser motivo de algum tipo de discriminação ou restrição de liberdade, sendo assim, o legislador achou por bem definí-los em uma categoria própria, com um manejo mais rígido.

Já o outro tipo de dado mencionado se relaciona com o dado anonimizado, que seja, um dado em que já não é mais possível haver a identificação de seu titular, nesse caso também o legislador previu uma liberdade maior para com estes dados.

Em seguida podemos citar os seguintes incisos do artigo 5º:

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;

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

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

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Neste ponto surgem as definições de quem irá realizar o tratamento destes dados, inclusive, define também o que vem a ser o “tratamento”, que seja, as movimentações, armazenamento, movimentações, transferências e outros procedimentos com os dados do titular.

Além disso nomeia que serão os responsáveis por tal realização, que seja, o controlador e o operador de dados, ambos podendo ser pessoa física ou jurídica, de direito público ou privado, sendo a diferenciação que o controlador é responsável pelas decisões referentes aos dados, e o operador por realizar o tratamento destes.

Por fim também dá uma definição necessária ao “consentimento” já que este é um dos caminhos para se realizar o tratamento de dados do titular, colocando como requisitos ao consentimento ser uma “manifestação livre, informada e inequívoca”, como explicado a sua importância por Maciel (2019):

No entanto, o consentimento só é válido se atender inúmeros requisitos legais, o que o torna um ônus desnecessário caso o tratamento possa ser validado em uma das outras nove bases previstas no artigo 7º, sem falar que ao titular é garantido o direito de revogação a qualquer tempo. O consentimento, para ser válido, deve ser livre, informado e inequívoco, fornecido por escrito ou outro meio que demonstre a manifestação da vontade do titular, em cláusula destacada, sem vício de consentimento e referir-se a finalidades determinadas. Autorizações genéricas são consideradas nulas. Caixas de seleção pré-marcadas também são consideradas não legítimas, invalidando o consentimento. O controlador

deve adotar mecanismos eficazes para poder provar o consentimento obtido, uma vez que o ônus da prova é seu, conforme teor do disposto no §2º do art.

Tendo tais parâmetros de norte é possível discorrer mais sobre a lei em si, custa informar que a lei embora venha sob uma visão ligada ao digital e ao cenário do século XXI, ela não irá regular apenas dados digitais, ou seja, a lei foca no direito à proteção de dados em si, não no instrumento que ele será usado, como demonstra o seu artigo 1º:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O artigo 2º da lei traz as suas previsões dos fundamentos, importante ressaltar o prestígio dado à defesa do consumidor, ao se enquadrar entre estes, seguem os fundamentos da LGPD:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Já no artigo 3º é possível notar outro fator empoderador da LGPD, e inspirado no GDPR, que é o caráter de seguir o dado de foi coletado no Brasil, que seja, mesmo que o dado seja tratado em outro país, caso seja de um titular situado em solo brasileiro, haverá regulação da lei de proteção de dados:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

Em ato contínuo o artigo 4º prevê as possibilidades de exclusão da aplicação da LGPD, vejamos:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;~~

~~b) acadêmicos; (Redação dada pela Medida Provisória nº 869, de 2018)~~

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Ou seja, as opções de exclusão são de acordo com o inciso I, para os casos em que essa coleta seja realizada por pessoa física e para fins não econômicos, devendo estar ambos requisitos presentes. Para o inciso II, em caso de fins jornalísticos, artísticos e acadêmicos. Para o inciso III, segurança pública, defesa nacional, atividades de investigação criminal e que seja provenientes de fora do território nacional de acordo com o inciso IV.

Outro ponto fundamental da LGPD são os seus princípios, esses estão definidos da seguinte forma:

- princípios da finalidade, visando que os usos dos dados tenham propósitos legítimos e adequados;
- adequação, que este tratamento siga as diretrizes da finalidade dada;
- necessidade, para que os dados coletados sejam somente os necessários, sem fazer jus a coletar dados em demasia do titular;
- livre acesso, garantindo o fácil e gratuito acesso do titular aos dados que a parte mantenha;

- qualidade dos dados, a garantia dada ao titular da coleta correta dos dados, pois em diversas situações a sua desatualização ou incorreção pode acarretar em prejuízos ao titular;
- transparência, garantia ao titular de que as informações lhe dadas para consulta serão de fácil compreensão;
- segurança, a utilização de técnicas de segurança para proteção dos dados dos titulares;
- prevenção, utilização de técnicas para prevenção de danos aos dados dos titulares;
- não discriminação, não é possível a utilização dos dados para discriminação ou abuso para com o titular;
- responsabilização e prestação de contas, responsabilidade do agente de tratamento da demonstração de utilização de métodos seguros no tratamento dos dados.

No artigo 7º estão as disposições acerca das possibilidades de tratamento dos dados, o artigo elenca 10 possibilidades em seus incisos para o tratamento dos dados pessoais, os dados sensíveis terão previsão em artigo diverso devido a sua categoria específica, são eles:

- com a realização da manifestação de consentimento pelo titular, lembrando que já no artigo 5º a consideração dos requisitos do consentimento válido;
- em caso de obrigação legal ou de obrigação de regulação pelo controlador;
- quando for utilizado pela administração pública, para a execução de políticas públicas previstas em leis, regulamentos, contratos, convênios etc;
- quando forem utilizados por órgão de pesquisa, e mantendo sempre que possível, a anonimização dos dados pessoais;
- quando for requisito para a execução de um contrato em acordo com o titular dos dados;
- quando for necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

- em caso necessário para a proteção da vida ou da segurança física do titular ou de outrem;
- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- quando for necessário para atendimento de legítimo interesse do controlador, salvo em caso de violação dos direitos e garantias fundamentais do titular;
- em caso de proteção do crédito;

Para os casos onde o objeto tratado são os dados sensíveis, haverá uma previsão específica no artigo 11º da LGPD, mantendo certos pontos já trazidos, excluindo algumas possibilidades de uso e trazendo novas formas também. Nesse caso, as bases legais do artigo 7º irão se repetir, mas com a exclusão das possibilidades de utilização dos dados sensíveis para a execução de contrato, utilização para proteção de crédito e na alegação de legítimo interesse do controlador. Por outro lado é acrescentada a hipótese de utilização em caso de garantia de prevenção à fraude.

O regramento da LGPD acaba por gerir as diversas possibilidades de ações que podem vir a ser tomadas em relação aos dados pessoais, e foca também em garantir os direitos do titular, já que este, via de regra é apenas um usuário de determinado serviço frente a empresas gigantescas.

O artigo 17º da mesma lei elenca diversos direitos do titular dos dados, dentre eles, a confirmação dos dados junto ao controlador, a anonimização, a correção, eliminação, revogação do consentimento etc. Dessa forma há um grande poder ao titular, pois os dados mesmo que sob o banco de dados de um terceiro, ainda assim lhe pertencem e uma das formas de realizar a fiscalização dessas questões será por meio da Agência Nacional de Proteção de Dados. Assim haverá uma entidade estatal responsável pela verificação do cumprimento da legislação pertinente.

Portanto, enquanto regularização de normas sobre as políticas de privacidade e proteção de dados vemos que há preocupação social e estatal, refletidas na legislação mencionada. Todo esse processo visa adequar a realidade da proteção de dados posta como desafio global na atualidade, em um mundo com diversas

ameaças legais, desde da invasão de sua privacidade por empresas em contratos não lidos, as “políticas de privacidade” ao se inscrever em um site, até a risco de algum de seus dispositivos ser invadido, gerando uma situação em que o indivíduo se tornará refém digital de outrem.

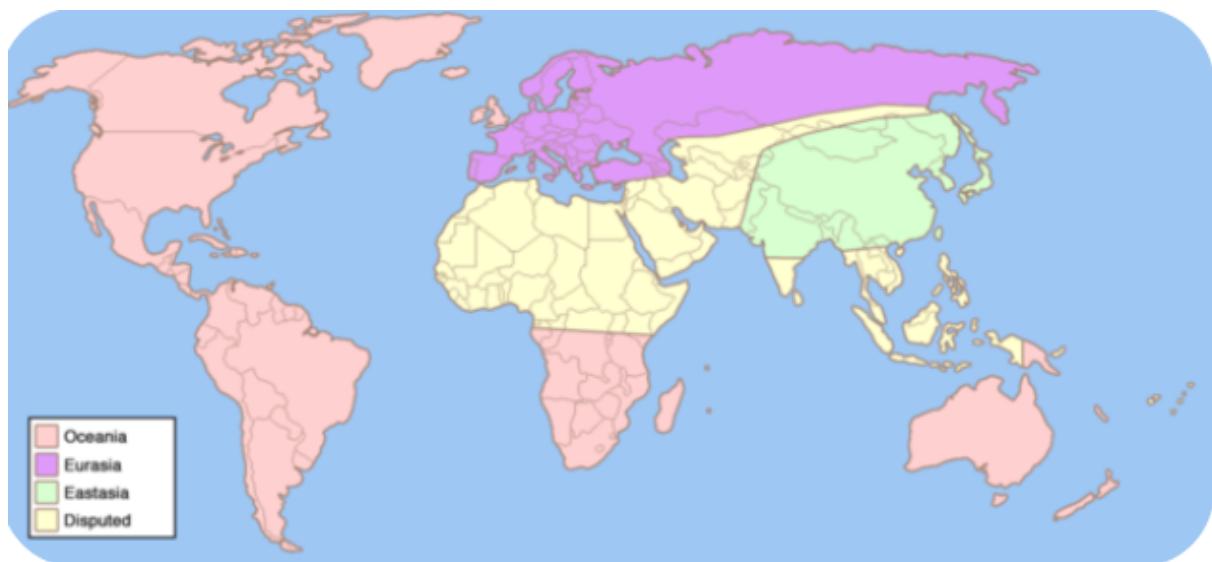
Dessa forma a passagem de forma breve pela legislação nacional visa elencar um pouco quais são as principais questões sobre as possibilidades de uso dos dados e do seu respeito às garantias individuais do indivíduo, tendo como norte a menção de como a proteção de dados é tratada no Brasil atualmente, e qual rumo essa área está tomando. Servindo assim de parâmetro da realidade nacional frente à comparação literária, e os desafios apresentados pelas novas tecnologias já mencionadas.

3 - A PRIVACIDADE DOS DADOS SOB A ÓTICA DE “1984”

3.1 - Contexto da Obra

1984 é um livro escrito pelo inglês George Orwell em 1949, em que o autor explana a possibilidade de existência em uma sociedade dominada pelo autoritarismo político e social. Tal sociedade é encarnada no personagem principal da obra, Winston Smith, que é funcionário do Ministério da Verdade, onde ironicamente, ele é responsável por reescrever notícias, criando assim, novas verdades. Seu país, Oceania, é um dos poucos países existentes que dividiram o mundo entre si e tem um estado de guerra constante.

Imagen 2 - Mapa mundi na obra “1984”



Nessa sociedade coletivista em que o indivíduo é nada mais que uma ovelha pastoreada, há um grande pastor, o grande irmão, o big brother é o líder da revolução que mudou Oceania para esse novo estágio de sociedade. A sociedade é dividida da seguinte forma:

the entire apparatus of government was divided: the Ministry of Truth, which concerned itself with news, entertainment, education, and the fine arts; the Ministry of Peace, which concerned itself with war; the Ministry of Love, which maintained law and order; and the Ministry of Plenty, which was

responsible for economic affairs. Their names, in Newspeak: Minitrue, Minipax, Miniluv, and Miniplenty.

Orwell (1977)

Porém, mesmo dentro dessa realidade esmagadora, sem controle de sua privacidade, das informações que consome, ou até mesmo da língua que fala, já que um dos objetivos da sociedade é criar uma nova língua, em que até mesmo pensar contra o regime seja algo impraticável, Winston pensa em resistir, como mencionado por Pavloski (2014):

É possível perceber em 1984 certo grau de infantilização ao qual estão expostos todos os indivíduos. O condicionamento psicológico e físico imposto pelo regime totalitário não só automatiza os sujeitos, como também os obriga a viver em um constante estado de terror sustentado por regras rígidas e por violentos dispositivos punitivos.

Sua história muda ao conhecer Julia, uma jovem também participante do partido, que desperta em Winston o desejo pelo novo e pela liberdade levando o protagonista a situações de desafio ao regime, mesmo que grande parte desses atos sejam uma questão de foro íntimo.

Ao fim, como o enredo distópico poderia indicar, não há um final necessariamente feliz, Winston é preso pelo regime e levado a um regime de torturas e readequação mental, não havia vontade do partido de matá-lo simplesmente, mas sim de adequá-lo socialmente, e após o longo processo de torturas chegando até a temida sala 101, é o que acontece, o herói sucumbe e desiste de seu amor quase revolucionário.

A sua revolta solitária serve, em grande medida, para salientar não apenas o nível de controle exercido pelo Estado, mas também o grau de alienação a que os indivíduos devem ser submetidos em nome do equilíbrio alcançado na Oceania. Diante desse contexto, Winston Smith tenta preservar a liberdade no único espaço que lhe resta: sua própria mente. Entretanto, o poder exercido na distopia orwelliana ultrapassa o plano físico e atinge camadas mais profundas da psique humana.

Pavloski (2014)

Outro ponto essencial para a situação vivida por Winston é controle político que há na sociedade, não existem partidos, e apenas a voz do grande irmão é ouvida, toda a sociedade é compostos de quase autômatos que não a capacidade de decidir o que ver, consumir, conversar ou agir.

Todo esse controle é posto em oposição a uma figura quase mítica, Goldstein, que em uma comparação simples estaria para o grande irmão, assim como Trotsky estava para Stalin, uma figura que até onde se recorda tinha um importante papel na revolução, mas que entrou em desgraça no partido e fugiu, servindo hoje de justificativa para diversas perseguições, pois o mesmo estaria organizando uma resistência ao regime, como mencionado por Orwell (1977):

Goldstein was the renegade and backslider who once, long ago (how long ago, nobody quite remembered), had been one of the leading figures of the Party, almost on a level with Big Brother himself, and then had engaged in counter-revolutionary activities, had been condemned to death, and had mysteriously escaped and disappeared.

Não sendo essa a única vez que o autor constrói personagens semelhantes à história da ditadura comunista na União Soviética, tão clássica e parecida quanto, é a relação de Bola de Neve e Napoleão como citado em Orwell (2020) , os dois porcos antagonistas, sendo este antagonismo criado por Napoleão, que começa a acusar Bola de Neve de sabotagem após expulsá-lo.

Importante ressaltar que parte do conceito proposto dessa distopia está intimamente ligada à extinção da existência de vida privada, como mencionado por Pavloski (2014):

Segundo esses autores, dos quais George Orwell é de nosso especial interesse, a implementação de uma sociedade idealizada sob a égide de uma doutrina universalizante é, em sua própria natureza, uma distopia, uma vez que desrespeita a individualidade e desconsidera todo e qualquer ponto de vista não concomitante com seus próprios dogmas.

Para entendermos a situação da privacidade no universo de Oceania é necessário entender a visão do protagonista e sua rotina, toda a sua rotina é ditada por membros superiores e impessoais do partido, além da figura quase celestial do grande irmão.

Winston, como um representante de seu tempo é apenas um ser sem voz, em que tudo que consome é decidido pelo partido, sem uma real opção de escolha, essa situação nos traz a realidade vivida pelo personagem, que é consumidor de propaganda governamental a quase todo momento:

Em princípio, um membro do Partido não tinha horas vagas, e não ficava nunca só, exceto na cama. Supunha-se que quando não estivesse

trabalhando, comendo ou dormindo, devia participar de alguma recreação comunal; era sempre ligeiramente perigoso fazer qualquer coisa que sugerisse o gosto pela solidão, mesmo que fosse apenas passear sozinho. Pavloski(2014. ORWELL, 2003, p. 83).

Essa é a vida de Winston, uma sociedade ideológica onde as opiniões não eram emitidas, apenas recebidas, sendo o ser humano o receptador de todo esse conteúdo de uma via só. Como mencionado por Pavloski (2014) a sociedade de vigilância era uma constante, não unicamente em razão do uso da tecnologia, mas com auxílio dela:

O primeiro aspecto a chamar a atenção na leitura do romance é a eficaz vigilância mantida ininterruptamente sobre a população. Esse mecanismo se manifesta de diferentes formas, algumas mais sofisticadas no sentido tecnológico e outras mais intimamente ligadas a fatores ideológicos que sustentam o poder estatal em 1984

Esse pensamento não é unicamente trazido por Pavloski, tendo ele mais companheiros de academia que adentram na mesma visão.

Jeffrey Meyers acredita que, dentro dessa proposta narrativa primordialmente política de Orwell em 1984, a valorização exagerada do papel da tecnologia suavizaria o extremo poder sustentado pelo Partido, uma vez que seriam incluídos outros fatores de condicionamento social.

Mas embora haja o debate acerca de qual fator é o mais preponderante na obra de Orwell, tanto a sociedade de vigilância em razão da tecnologia, quanto a opressão política, estarão entre os principais temas. As técnicas de controle social utilizadas pelo sistema de Oceania também tem como efeito colateral o dano à privacidade, seja a constante propaganda que tem que ser escutada ou vista a todo momento, seja até mesmo a Novalíngua (reforma no idioma utilizado em Oceania de forma impossibilitar pensamentos contrários ao governo), que em última análise é a tentativa de acabar com a privacidade dentro da mente do protagonista.

Acabando assim com o próprio sentido da comunicação, como mencionado por Ferraz (2019), a língua é composta por signos que tem a sua relação com a realidade definida pelo homem, e cabendo a consideração ao uso que cada comunidade dará a estes signos, ocorre que, o sentido de Novalíngua acaba com o fator do uso social, ao moldar o significado que deverá ser dado e utilizado pelo cidadão.

E qual seria então o papel da tecnologia nesse mundo distópico? Bom, uma das principais ferramentas utilizadas pelo partido em 1984 para o controle social dos cidadãos é algo que tinha um teor surreal em 1949, quando Orwell a escreveu, mas que hoje tem uma visão perigosamente familiar, as teletelas.

As teletelas são como televisões, que os cidadãos e funcionários do governo em Oceania tinham em suas casas, ocorre que ela tinha algumas peculiaridades, primeiro, não haviam opções, toda a programação estava sempre focada em propaganda política encabeçada pelo Grande Irmão.

Além disso, todos os ambientes, compartilhados ou particulares, funcionam como espaços de análise comportamental e ideológica. O olho do poder destrói completamente o conceito de solidão. Pode-se dizer que as celas do Panóptico equivalem ao universo pessoal dos cidadãos da Oceania. No universo ficcional, o olhar do inspetor é substituído por aparelhos que captam, ao mesmo tempo, sons e imagens: as teletelas.

Pavloski (2014)

Outro fator próprio desse meio de entretenimento reverso é que a sua função não era apenas permear a residência de quem a tinha com propagandas políticas todo o dia, e ser assistida pelo residente, mas sim assistir, afinal, a teletela via tudo e escutava tudo, sendo assim um aparelho espião declarado aos cidadãos, lhe privando de qualquer possibilidade de liberdade ou privacidade, até mesmo em seu recinto mais íntimo, Pavloski (2014) demonstra a situação:

As teletelas são encontradas em praticamente todos os lugares, de maneira que o indivíduo esteja em casa, no trabalho e mesmo na cama, a observação nunca é interrompida. Ainda que existam divisões hierárquicas dentro do próprio Partido, nenhum cidadão está livre do olhar frio da pequena placa de metal, mesmo aqueles que têm como função vigiar os seus compatriotas.

Sendo assim é possível a conclusão de que a privacidade na obra do autor inglês era quase nula, afinal, câmeras monitoram cada instante do autor, até mesmo em sua residência, o ouviam, e avaliavam tudo o que o mesmo fazia, deixando-o em uma situação da mais completa fragilidade, onde o simples comando do cérebro ao corpo deve ser reprimido, pois ele sempre estará vigiado.

3.2 A realidade da década 2020 frente às perspectivas traçadas por Orwell

E sobre esse ponto deverá ser feita a análise no presente estudo, afinal, como estava retratada a situação da privacidade e de coleta de dados dos habitantes dessa Londres distópica de 1984, e o quanto próxima ela está da nossa sociedade em 2020.

A comparação não é mera liberdade textual, mas uma analogia fática, afinal como mencionado por Mayer-Schonberger e Cukier (2013, p. 150)In 2007 the British media relished the irony that there were more than 30 surveillance cameras within 200 yards of the London apartment where George Orwell wrote 1984.

Ou seja, essa comparação demonstra o estágio que atingimos, um cenário digno de uma distopia do pós guerra. A própria ideia de privacidade em muitos casos já foi retratada como um obstáculo, seja na distopia de Orwell, ou até mesmo em literaturas utopistas, como citado por Pavloski (2014):

Grande parte das sociedades utópicas apresenta como característica um rígido controle das ações individuais como forma de manutenção da estabilidade alcançada. Para esses autores, o modelo utópico se baseia, em grande medida, na uniformidade política e ideológica de seus cidadãos. Não basta desejar o paraíso social, os indivíduos devem oferecer sacrifícios pessoais para que a ordem seja preservada. As decisões políticas são centralizadas no soberano ou em um reduzido grupo de legisladores, cabendo aos demais membros do grupo o atendimento irrestrito aos desígnios dos líderes do Estado. Por exemplo, em A Nova Atlântida, de Francis Bacon, a vida dos cidadãos é direcionada e vigiada por uma instituição chamada Casa de Salomão.

Afinal, em mundo tão tecnológico como o nosso, onde a localização das pessoas foi até mesmo utilizada para tentar rastrear possíveis transmissores de Covid-19, é possível pensar que qualquer forma de privacidade seria uma fuga da justiça ou razão de esconder algum crime.

Ocorre que, Orwell nos traz a perspectiva reversa, afinal, o que hoje é a realidade, poderá não ser mais em um futuro a curto ou médio prazo, se hoje a

quebra da privacidade é usada para rastrear doenças, qual garantia tem-se de que não será usada para outros fins à frente?

Ou seja, o risco constante de que os direitos adquiridos, caso não sejam vigiados, venham a ser perdidos em momentos futuros, na realidade da obra, para um governo totalitário.

Em um primeiro momento a análise da realidade frente a obra poderá ser vista em relação a governos totalitários ou autoritários, como a Alemanha Nazista ou Ditadura Soviética, que, caso ainda existissem usariam da tecnologia para tornar a realidade de perseguição à sua população ainda maior. Dessa forma 1984 pode ser visto como uma previsão um tanto quanto pessimista, mas representando o momento e a realidade do autor.

George Orwell nasceu no começo do século XX, e escreveu 1984 em 1949, pouco tempo após a derrocada da Alemanha nazistas, não dos regimes totalitários em si, já que um outro estado policial e ditatorial aumentava sua influência no mundo, a União Soviética.

Sendo assim, ele refletiu aflições de sua época, questões que tratavam sobre o que aquele tipo de governo faria com o aumento da capacidade de controle social da população. É clara a visão de que se os nazistas pudessem à época ter tatuado um QR code nos judeus dos campos de concentração ao invés de apenas seu número, constando toda a ficha, nome, profissão, histórico político etc, eles o fariam.

Um exemplo de situação passível de acontecer na visão de um estado gigantesco é o sistema de pontuação à população planejada na China. Porém, mesmo considerando o temor relacionado ao crescimento do poder estatal, a realidade nos mostra que o mundo acabou por não se tornar necessariamente uma Oceania. Pois, diferentemente do retratado na obra, em grande parte do mundo os regimes totalitários caíram, após o fim da Alemanha nazista e da Itália fascista em 1945, os regimes com tendências fascistas remanescentes na Europa ocidental caem, Portugal em 1974, e a Espanha em 1975. Já ao fim dos 80 há a caída do

bloco do leste europeu, onde haviam diversas ditaduras comunistas, como a Romênia, Hungria, Alemanha Oriental etc, e ao fim a própria União Soviética.

Dessa forma, a maioria das nações que planejavam um sistema de estado controlador da sociedade e ditatorial, acabaram por cair antes da difusão do uso de GPS, gravadores de voz, filmadoras, tudo isso em um único aparelho, portátil e difundido nas mais diversas classes, o Smartphone. Em contrapartida alguns dos regimes totalitários sobreviventes inibiram ao máximo a difusão da tecnologia e acesso à internet em seus territórios, como o caso de Cuba e da Coréia do Norte.

Com exceção da China, nenhum outro regime parece tão próximo da sociedade de Oceania, onde há controle em larga escala do que é possível ou não ser pesquisado ou assistido. Afinal nunca é tarde para lembrar que os serviços do Google são bloqueados da China, que incluem Gmail, Youtube etc, além de outros populares sites e apps do mundo, como Facebook, Instagram, Whatsapp, Twitter (SUMMERS, 2020).

E, embora esse controle seja fruto da natureza política chinesa, uma ditadura comunista de partido único, ainda assim está mares de distância da projeção de Orwell, já que ainda há acesso a internet, certa liberdade em comunicação, e, embora tenham sido feito denúncias acerca da instalação de câmeras dentro da casa de pacientes com Covid-19 (GAN, 2020) para garantir que os mesmos estão cumprindo a quarentena, ainda é possível verificar a larga distância da China até Oceania.

Por outro lado a realidade das teletelas não é distante também dos habitantes dos países não ditoriais, afinal, superando a visão de Orwell nossa sociedade desenvolveu uma teletela portátil, que nos escuta 24 horas por dia, 7 dias por semana, e onde tanta parte de nossa vida está inserida que soa quase impossível abandoná-la, isso mesmo, os celulares, como mencionado por Lanier (2018):

Os algoritmos se empanturram de dados sobre você a cada segundo. Em que tipos de link você clica? Quais são os vídeos que vê até o fim? Com que rapidez pula de uma coisa a outra? Onde você está quando faz essas coisas? Com quem está se conectando pessoalmente e on-line? Quais são as suas expressões faciais?

Ou seja, a realidade transformou o Grande Irmão, no “Pequeno Irmão”, que nos acompanha e vigia a todo momento, mas nesse caso, muitas vezes não se dá conta que se está sendo vigiado, e não há no geral a consciência de risco caso se dê conta.

A sociedade atual gera mais dados do que nunca, e mais informações sobre seus cidadãos do que Stalin jamais imaginou. A grande diferença até o momento demonstrada pelo exposto acerca da realidade de 1984 para 2020, não é necessariamente a exposição da vida do indivíduo a um terceiro, e a eventual influência que este poderá ter no seu dia, mas sim quem é esse terceiro.

Sendo assim, a vigilância está aí, cada vez mais presente, mas mesmo com o número de câmeras policiais nas cidades aumentando, ainda é muito menor que as câmeras privadas, e quem as vigia?

A mesma pergunta serve para outras questões, até mesmo sobre o controle de com quem nos relacionamos, como mencionado por Magrini (2019):

Tendo em vista a descrição prévia sobre o funcionamento dos negócios digitais baseados em dados e dos efeitos do filtro-bolha, a ideia de que a infraestrutura da internet como esfera pública tem o potencial de permitir que as discussões possuam força suficiente para chegar a diferentes segmentos e a grupos de interesses diversos, replicando-se pelas várias redes de pessoas que compõem a sociedade, talvez seja uma realidade cada vez mais distanciada. Isso se deve ao fato de que as expressões ficam muitas vezes restritas a uma mesma rede de pessoas com interesses comuns e com canais de comunicação facilmente manipuláveis pelos detentores das plataformas. A consequência disto é a intensificação da fragmentação comunicacional e a polarização do debate público.

Portanto, é possível fazermos a relação do pensamento exposto por Orwell frente a realidade de 2020, mas alguns dos participantes do jogo parecerão trocados, afinal, não há uma Grande Irmão hoje, mas sim vários, os grandes membros do mercado de produção e manipulação de dados, Facebook e Google como maiores exemplos disso, pela extensão de suas conexões, afinal ambos são conglomerados de várias empresas que permeiam nosso dia a dia. Um exemplo claro dessa situação é demonstrado pelo google maps, uma simples procura por “google time line” na internet leva a um link que mostra onde o indivíduo esteve todos os dias com o seu celular, desde quando ele tem registro, a função presente

no sistema Android pode pegar muitos de surpresa, mas é pura prova de que ao longo dos últimos anos havia sempre um “Pequeno Irmão” acompanhando todos os passos dados e armazenando-os.

E essa é a realidadeposta até o momento, cada vez mais conectados ao mundo, os indivíduos muitas vezes não sabem sequer para onde vão, afinal o nível de controle que será possível chegar ao longo dos próximos anos será cada vez mais distante do imaginado na época de Orwell, o século XXI, embora com liberdade poética e sem ficar preso totalmente ao roteiro, transformou uma distopia em realidade.

5 - CONSIDERAÇÕES FINAIS

Em que ano estamos, 1984 ou 2020? O trabalho ora tratado buscou trazer as particularidades de cada um, mostrando o quanto foi possível a sociedade evoluir nos últimos 60 desde a obra de George Orwell.

O escritor inglês conseguiu a seu tempo, vislumbrar algumas das novidades tecnológicas que seriam trazidas ao longo dos anos, a própria teletela é um exemplo disso, o dispositivo que poderia parecer de uma intromissão surreal na vida privada em 1949, mas que são tratados com trivialidade em 2020.

Em certos aspectos até mesmo superamos o sonho distópico do livro, afinal, o conceito de Big Data e Internet das Coisas, coletando dados a todo momento e realizando uma experiência personalizada, que também pode acabar em manipulação, vem por um caminho macio, do que o proposto no livro, em que há a necessidade da estruturação de maquinário passando uma única programação com fins de convencimento da população.

2020 não é 1984, 2020 pode ser até mais eficaz no convencimento, afinal a realidade de conversar próximo ao celular sobre algum bem que se quer comprar ou viagem a fazer, e ao entrar nas redes sociais se deparar com um anúncio do mesmo objeto pode soar muito conveniente.

Da mesma forma a criação de bolhas nas redes sociais, onde os algoritmos muitas vezes direcionam a interação apenas com pessoas que concordam entre si, baseada nos interesses, pode acarretar em uma radicalização de diversos assuntos, mas ainda assim muito mais sutil que o Grande Irmão de Oceania.

A arte até mesmo reflete a realidade, muito conhecido no Brasil é o reality show Big Brother Brasil, uma experiência onde diversas pessoas vão se isolar em uma casa, com câmeras em todos os cômodos 24 horas por dia por alguns meses.

Ocorre que mais uma vez a realidade evoluiu mais que a ficção, hoje a ida ao Big Brother não soa mais como um período de extrema vigilância saindo da vida pacata na sociedade, em muitos casos pode ser na verdade um período de afastamento do digital, do celular, das redes sociais. Pois na “casa mais vigiada do Brasil” a única vigilância é a das câmeras, não há a relação quase umbilical de um indivíduo com as redes sociais, com aparelhos lhe oferecendo propagandas a todo momento com base nos seus dados etc.

Essa reflexão leva a conclusão de que a sociedade não ficou menos tecnológica que o previsto em 1984, ficou mais até. O que muda é que não há (até o momento) o uso político massivo destes instrumentos, quem nos vigia e armazena nossos dados não é o governo, mas as empresas de quem consumimos produtos, o capitalismo está 4.0.

Ainda assim as reflexões de Winston servem como uma previsão pessimista, mas não impossível de um futuro que ainda virá, quiçá em 2084, os instrumentos de controle já estão presentes.

Os clássicos não são lidos apenas para divertimento, mas para entender as relações na sociedade, e por isso a obra do autor inglês é tão importante, fazer a conversa entre nossa sociedade e seus próprios problemas com os propostos no livro leva a um momento de abstração de até onde é possível ir e quais são as tentativas de regular a situação na sociedade digital.

REFERÊNCIAS

ALCANTARA, Larissa Kakizaki. **Big Data e IoT: Desafios da privacidade e da proteção de dados no direito digital.** 1. ed. São Paulo. ebook. 2017.

Banco Mundial. **PIB dos Países.** Disponível em <https://www.google.com/publicdata/explore?ds=d5bncppjof8f9_&met_y=ny_gdp_m_ktp_cd&idim=country:BRA:ARG:ITA&hl=pt&dl=pt> Acesso em 25 de nov. 2020.

BBC. **German parents told to destroy Cayla dolls over hacking fears.** Disponível em: <<https://www.bbc.com/news/world-europe-39002142>> Acesso em 18 de nov. 2020.

BOSWORTH, A. B. **Athens and Melos.** Disponível em <<https://www.encyclopedia.com/international/encyclopedias-almanacs-transcripts-and-maps/athens-and-melos>> Acesso em 25 de nov. 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 21 nov. 2020.

BRASIL. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 19 de nov. 2020.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. **Institui o Código Civil.** Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 18 de nov. 2020.

BRASIL. Lei 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências.** Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 18 de nov. 2020

BURKE, Minyvonne. **Amazon's Alexa may have witnessed alleged Florida murder, authorities say.** Disponível em <<https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621>> Acesso em 26 de nov. 2020.

CARLOTTO, Maria Caramez. **Acesso negado: Propriedade intelectual e democracia na era digital.** 1. ed. Edições SESC, ebook. 2019.

CARDOSO, Carlos. **A Internet das coisas (inutéis) egg minder.** Disponível em: <<https://tecnoblog.net/meiabit/271383/thinkgeek-egg-minder-smart-bandeja-pra-ovo/>> Acesso em 15 de nov. 2020.

EVANS, Dave. **The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.** Cisco Internet Business Solution Group. Disponível em: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IOT_IBSG_0411FINAL.pdf> Acesso em 14 de nov. 2020.

FANKHAUSER, Jarrod. **China's society credit system is pegged to be fully operational by 2020 - but what will look like?.** Disponível em <<https://www.abc.net.au/news/2020-01-02/china-social-credit-system-operational-by-2020/11764740>>. Acesso em 18 de nov. 2020.

FREITAS, Eduardo. **Crescimento da população Mundial.** Disponível em <<https://mundoeducacao.uol.com.br/geografia/crescimento-populacao-mundial.htm#:~:text=Ap%C3%B3s%201.600%20anos%2C%20a%20soma,ultrapassava%20500%20milh%C3%A3es%20de%20habitantes.&text=Em%201850%2C%202000%20anos%>>

20depois,atingiu%201%20bilh%C3%A3o%20de%20pessoas.&text=De%201850%20a%201950%200,2%2C5%20bilh%C3%B5es%20de%20habitantes.> Acesso em 26 de nov. 2020.

GAN, Nectar. **China is installing surveillance cameras outside people's front doors...and sometimes inside their homes.** Disponível em <<https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html>> Acesso em 15 de nov. 2020.

IBGE. **População do Brasil.** Disponível em <https://www.ibge.gov.br/apps/populacao/projecao/box_popclock.php> Acesso em 16 de nov. 2020.

IBGE. **CONCLA - Comissão Nacional de Classificação.** Disponível em: <[https://cnae.ibge.gov.br/en/component/content/article/290-teen/censo/censo-2000/1703-o-censo-tem-historia.html#:~:text=Os%20romanos%20fizeram%2072%20censo,s,respondia%20geralmente%20era%20a%20morte!](https://cnae.ibge.gov.br/en/component/content/article/290-teen/censo/censo-2000/1703-o-censo-tem-historia.html#:~:text=Os%20romanos%20fizeram%2072%20censo,s,respondia%20geralmente%20era%20a%20morte!>)> Acesso em 19 de nov. 2020.

LANIER, Jaron. **Dez argumentos para você deletar agora suas redes sociais.** 1. ed. Intrínseca, ebook. 2018.

LA BOETIE, Etienne De. **Discour de la Servitude Volontaire.** ebook.

MACIEL, Rafael. **Manual Prático Sobre a Lei Geral de Proteção de Dados:** Atualizado com a Medida Provisória nº 869/18. 1. ed. Goiânia. RM Digital Education, ebook. 2019.

MAGRINI, Eduardo. **A Internet das Coisas.** 1. ed. FGV, ebook. 2018.

MAGRINI, Eduardo. **Entre Dados e Robôs: Ética e privacidade na era da hiperconectividade.** 2. ed. Arquipélago Editorial, ebook. 2019.

MARTINEZ, Javier Garcia. **Here's what will happen when 30 billions devices are connected to the internet.** Disponível em: <<https://www.ge.com/news/reports/heres-what-will-happen-when-30-billion-devices-a-re-connected-to-the-internet>> Acesso em 15 de nov. 2020.

MALDONADO, Viviane Nóbrega. **Advocacia 4.0.** 1. ed. Revistas dos Tribunais, ebook. 2019. MARY, Beard. **Uma História de Roma Antiga.** Crítica, 2017. ebook.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big Data:** A revolution that will transform how we live, work, and think. London. John Murray, ebook. 2017.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e direito do consumidor** - Linhas gerais de um novo direito fundamental. 1. ed. Série IDP/Saraiva, ebook. 2017.

ORWELL, George. **1984.** Houghton Mifflin Harcourt. New York, ebook. 1977.

ORWELL, George. **Animal Farm.** ebook.

PAVLOSKI, Evanir. **1984: A distopia do indivíduo sob controle.** UEPG, ebook. 2014

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à lei n 13.709/2018 - LGPD. 2. ed. São Paulo, ebook. 2020.

NORDRUM, Amy. **Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated.** Disponível em: <<https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>> Acesso em 15 de nov. 2020.

ONU. **Declaração Universal dos Direitos do Homem.** Disponível em <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>> Acesso em 23 de nov. 2020.

POR EM MOVIMENTO. Brasileiro é um dos campeões em tempo conectado à internet. Disponível em <<https://g1.globo.com/especial-publicitario/em-movimento/noticia/2018/10/22/brasileir>>

o-e-um-dos-campeoes-em-tempo-conectado-na-internet.ghtml> Acesso em 25 de nov. 2020.

RUSHTON, Katherine. **Samsung Warns viewers: Our smart TVs could be snooping on your private conversations.** Disponível em <<https://www.dailymail.co.uk/sciencetech/article-2945766/Is-TV-eavesdropping-PRIVATE-conversations-Samsung-warns-users-smart-sets-capture-word.html>> Acesso em 26 de nov. 2020.

SAMPAIO FERRAZ, Tércio. **Introdução ao Estudo do Direito:** técnica, decisão, dominação 11. ed. São Paulo: Atlas, 2019. ebook.

SILVEIRA, Sérgio Amadeu. **Tudo Sobre Tod@s:** Redes digitais, privacidade e venda de dados pessoais. 1. ed. São Paulo. Edições SESC, ebook. 2017.

SUMMERS, JOSH. **List of Websites and Apps Blocked in China for 2020.** Disponível em <<https://www.travelchinacheaper.com/index-blocked-websites-in-china>> Acesso em 25 de nov. 2020.

TELECO. **Estatística de Celulares no Brasil.** Disponível em: <<https://www.teleco.com.br/ncel.asp>> Acesso em 16 de nov. 2020.

UNCTAD. **Data Protection and Privacy Legislation Worldwide.** Disponível em <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>> Acesso em 23 de nov. 2020.

WARREN, Samuel D.; BRANDEIS, Louis. **The Right to Privacy.** Quid Pro Laws Book, ebook. 2010.

WIMMER, Miriam. **Proteção de Dados Pessoais em uma economia movida a dados.** Disponível em <<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>> Acesso em 25 de nov. 2020.