CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ
CURSO DE BACHARELADO EM DIREITO

ARTHUR CLEMENTINO COSTA DE LEMOS
NEILA LORRANE SOUSA DA CUNHA

O DIREITO DE FICAR OFF-LINE: uma análise sob a ótica de garantia constitucional à privacidade e a Lei Geral de Proteção de Dados Pessoais - LGPD

BELÉM
2021

ARTHUR CLEMENTINO COSTA DE LEMOS
NEILA LORRANE SOUSA DA CUNHA

O DIREITO DE FICAR OFF-LINE: uma análise sob a ótica de garantia constitucional à privacidade e a Lei Geral de Proteção de Dados Pessoais - LGPD

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Profa. Me. Amanda Ramalho

BELÉM
2021

Dados Internacionais de Catalogação-na-publicação (CIP)
Biblioteca do CESUPA, Belém – PA

L557d Lemos, Arthur Clemetino Costa de.

O direito de ficar off-line: uma análise sob a ótica de garantia constitucional à privacidade e a Lei Geral de Proteção de Dados - LGPD / Arthur Clementino Costa de Lemos, Neila Lorrane Sousa da Cunha. - Belém, 2021.

27 p.

Trabalho de Conclusão de Curso (Graduação) – Centro Universitário do Estado do Pará, Bacharelado em Direito, Belém, 2021.

Orientadora: Profa. Ma. Amanda Maia Ramalho.

1. Direito à privacidade. 2. Brasil. Lei Geral de Proteção de Dados Pessoais (2019). I. Cunha, Neila Lorrane Sousa da. II. Ramalho, Amanda Maia (orient.). III. Título.

CDD 341.2738

Regina Coeli Araújo Ribeiro CRB-2/739

ARTHUR CLEMENTINO COSTA DE LEMOS
NEILA LORRANE SOUSA DA CUNHA

O DIREITO DE FICAR OFF-LINE: uma análise sob a ótica de garantia constitucional à privacidade e a Lei Geral de Proteção de Dados Pessoais - LGPD

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção de grau em Bacharel em Direito, pelo Centro Universitário do Estado do Pará.

Orientadora: Profa. Me. Amanda Ramalho

Data de aprovação: _____/_____/_____

Conceito:

Banca Examinadora:

_____
Profa. Me. Amanda Maia Ramalho - Orientadora
Centro Universitário do Estado do Pará (CESUPA)

_____
Nome com titulação
Instituição a que pertence

_____
Nome com titulação
Instituição a que pertence

O DIREITO DE FICAR *OFF-LINE*: UMA ANÁLISE SOB A ÓTICA DE GARANTIA CONSTITUCIONAL À PRIVACIDADE E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD.

THE RIGHT TO BE OFFLINE: AN ANALYSIS FROM A CONSTITUCIONAL PERSPECTIVE OF PRIVACY GUARANTEES AND THE GENERAL LAW FOR THE PROTECTION OF PERSONAL DATA.

Arthur Clementino Costa de Lemos [1]

Neila Lorrane Sousa da Cunha [2]

Orientadora: Amanda Ramalho[3]

RESUMO

A possibilidade de ficar "*off-line*" se distancia a cada dia, pois hoje o mundo gira em volta de coletagem de dados. O objetivo desse trabalho é mostrar os novos parâmetros da privacidade dos indivíduos nesse "novo" tipo de capitalismo, focado no titular dos dados, a fim de devolver a esse o poder de escolha e a opção de controlar os seus dados de forma transparente e dar o poder ao titular de escolher quais dados acha interessante compartilhar e como os mesmos vão ser utilizados. Este trabalho também levanta uma análise do contexto histórico do Direito à Privacidade e da Regulamentação Geral de Proteção de Dados para a criação da Lei Geral de Proteção de Dados. Neste trabalho foi realizado uma pesquisa bibliográfica a respeito da nova privacidade e como isso altera a maneira de como se deve encarar a coleta de dados de acordo com a LGPD. Ao final, o trabalho mostrará alternativas de como a sociedade pode controlar seus dados sem precisar ficar "off-line", e enfatizando que a LGPD é a ferramenta fundamental na defesa do titular, que garante o controle e a autonomia do indivíduo em relação aos seus dados.

Palavra-chave: Direito à Privacidade; Coleta de dados pessoais; Lei Geral de Proteção de Dados Pessoais.

ABSTRACT

The possibility of going "offline" is getting farther every day, as today the world revolves around data collection. The objective of this work is to show the new parameters of privacy of individuals in this "new" type of capitalism, focused on the data subject, in order to give back to them the power of choice and the option to control their data in a transparent way and give the power to the holder to choose which data he/she finds interesting to share and how it will be used. This work also raises an analysis of the historical context of the Right to Privacy and the General Data Protection Regulation for the creation of the General Data Protection Law. In this work, a bibliographic research was carried out regarding the new privacy and how it changes the way in which data collection should be viewed in accordance with the LGPD. At

[1] Graduando do Curso de Direito no Centro Universitário do Pará – CESUPA, turma DI10TB, e-mail: arthur11060250@aluno.cesupa.br.

[2] Graduanda do Curso de Direito no Centro Universitário do Pará – CESUPA, turma DI10TB, e-mail: neila19060406@aluno.cesupa.br

[3] Mestre em Direito pela UNAMA. Especialista em Compliance. LLC em Direito Empresarial no INSPER.

the end, the work will show alternatives on how society can control its data without having to go "offline", and emphasizing that the LGPD is the fundamental tool in the defense of the holder, which guarantees the control and autonomy of the individual in relation to the your data.
KEYWORD: Right to Privacy. Collection of personal data. General Personal Data Protection Law.

INTRODUÇÃO

A coleta de dados vem acompanhando diariamente a vida da humanidade, pois já se tornou cotidiano das empresas digitais e as tidas como “tradicionais” o uso destes para tomar decisões que afetam diretamente a vida dos usuários e consumidores.

Uma vez que a sociedade torna-se cada vez mais digital, onde uma ida ao supermercado gera dados relativos ao horário de visita, que tipo de produto é comprado primeiro nas gôndolas, quais produtos tendem a ser comprados em conjunto com outros, os dados ganham cada vez mais relevância. Por outro lado, a mesma facilidade ao acesso à informação que facilita a vida de muitos pode comprometê-los em outros pontos, visto que quanto maior for a sua utilização, mais exposta estará à privacidade de um indivíduo, na medida em que seus dados passam a ser processados, compartilhados e analisados massivamente, além de que esses dados são frequentemente recolhidos soturnamente, tratados de forma descentralizada e na maioria dos casos não há a devida transparência de como são utilizados ou coletados.

A pesquisadora Shoshana Zuboff cunhou o termo capitalismo de vigilância como a nova espécie de capitalismo, que as empresas aderiram devido a sua efetividade, em que os dados dos usuários são usados como matéria prima para a geração de capital, os pontos levantados pela autora: a coleta exponencial de dados como a matéria prima do capitalismo de vigilância, à análise cada vez maior de um volume de dados por *softwares*, e o armazenamento em conjunto com a distribuição sem regulamentação desses dados é relevante para demonstrar quais catástrofes nos aguardam caso não adotarmos medidas para corrigir a assimetria das relações titulares x controladores de dados e assegurar aos usuários que sua vida privada, escolha sexual, religiosa ou política não seja levianamente exposta.

Após a primeira revolução industrial a humanidade entrou em um *frenesi de progresso* no qual nunca havia experimentado. O ponto de inflexão que levou a essa aceleração, dentre outros, foi a capacidade de transformamos a matriz energética do animal para a mineral (carvão no primeiro momento e posteriormente petróleo e gás natural).

É dispensável mencionar todas as benesses oriundas dessa descoberta da energia a vapor, porém como consequências indesejadas dessa exploração tivemos desmatamento, mudanças climáticas, extinção de espécies, emissão desenfreada de gás carbono, acidificação dos oceanos. Essas inúmeras consequências são hoje um desafio para humanidade até hoje, pois há época não havia objeção a essa exploração desenfreada e desregulada, lidamos até hoje com problemas criados por essa geração que a solução hoje não é unânime ou sequer existe.

Portanto, fica evidente que a exploração da matéria prima, absolutamente necessária para a industrialização, gerou e gera até hoje não só perdas como desafios hercúleos que pesquisadores dedicam às vidas em busca da solução. Usando o passado como ponto de cabotagem para navegarmos em direção ao futuro, fica claro aqui a urgência deste trabalho na sua missão de propor alternativas para a proteção dos nossos dados uma vez que esses são a matéria prima do capitalismo de vigilância, utilizando-se da analogia do passado para encaramos o futuro; qual seriam as consequências de uma extração desenfreada dos nossos dados? O que seria do nosso futuro, quais "espécies" e "habitats" seriam afetados por essa nova era do capitalismo? Quantos danos seriam irreparáveis?

Não é o objetivo do presente trabalho responder essas questões, mas propor uma visão crítica sobre a privacidade e a coleta dos dados para que possamos refletir os novos parâmetros da privacidade dos indivíduos nesse "novo" tipo de capitalismo, focado no titular dos dados, a fim de devolver a esse o poder de escolha e opção de controlar os seus dados de forma granular e a capacidade de autoafirmação digital, isto é dar poder ao titular de escolher quais dados este acha interessante compartilhar e como os mesmos vão ser utilizados, reduzindo a assimetria na relação titular x controlador (LGPD).

Buscamos resolver a questão acima mencionada por meio de duas vertentes principais: primeiramente a análise da nova privacidade e como isso altera a maneira como deve-se encarar a coleta de dados, e em segundo lugar como podemos utilizar a Lei Geral de Proteção de Dados - LGPD como base para o direito de autodeterminação digital.Passaremos a entender também quais os dispositivos Constitucionais que se encaixam para garantir esses direitos e leis principalmente a LGPD, que embasam nossa égide de resguardar a garantia de privacidade do usuário.

1. O CAPITALISMO DE VIGILÂNCIA

1.1.Conceito

O termo capitalismo de vigilância foi cunhado pela pesquisadora Shoshana Zuboff, em seu livro "A ERA DO CAPITALISMO DE VIGILÂNCIA" de 2020, que por definição em suas próprias palavras:

> "1. Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para prática comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; 4. A estrutura que serve de base para a economia de vigilância; 5. Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX; 6. A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; 8. Uma expropriação de direitos humanos críticos que pode ser bem mais compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos."

Sem a intenção de desvirtuar as palavras da própria autora, cabe fazer uma simplificação do conceito *capitalismo de vigilância* para facilitar a compreensão dos que não tiveram a oportunidade de ler o livro da autora. *Capitalismo de vigilância* é a prática capitalista que busca, através da análise e processamento massivo dos dados produzidos na sociedade digital, prever comportamentos e vender tais previsões as empresas que por sua vez buscam oferecer aos consumidores exatamente o que eles desejam a fim de maximizar seus lucros. Assim complementa a pesquisadora Shoshana Zuboff (2020, p.13) que "o capitalismo de vigilância age por meio de assimetrias nunca antes vistas referentes ao conhecimento e ao poder que dele resulta. Ele sabe tudo sobre nós, ao passo que suas operações são programadas para não serem conhecidas por nós [...]".

O capitalismo de vigilância por sua própria definição e conceito é imperativamente desigual, as grandes empresas que coletam nosso dados (praticamente todas que desejam se manter competitiva no mercado atual) o fazem de uma forma soturna e não transparente, muitas vezes os usuários não tem conhecimento que cedem seus dados para tais empresas que se camuflam sob a égide de gratuitas para atrair usuários ao mesmo tempo que vendem os dados daqueles que utilizam seus serviços para quem oferecer mais, sem levar em consideração o que seria agradável para o usuário detentor dos dados. "As empresas começaram a explicar essas violações como um *quid pro quo* necessário em troca de serviços de internet "gratuitos"." (SHOSHANA ZUBOFF, 2020, p.72).

Sob a bandeira do serviço gratuito, emergem os mercados-futuros, onde a empresa rastreia nossos movimentos, cliques e tempo gasto em determinada ação para a definição de

um perfil (*profiling*) individualizado de nossos gostos, tendências de compra, preferências e até mesmo predisposições que o próprio usuário não percebe de forma consciente.

Os modelos preditivos (*softwares*) do capitalismo de vigilância são capazes de entender e criar um padrão para a experiência humana melhor do que um analista humana quando tenta compreender um paciente, a eficiência é tão assustadora que o caso paradigmático da Target (empresa americana de varejo) é até hoje objeto de debate, no caso o software da empresa Target foi capaz de prever que uma adolescente estava grávida por meio do seu padrão de compra das últimas semanas, e começou a enviar para a mesma diversos anúncios de fraldas e carrinhos de bebe, antes mesmo da própria gravida ter descoberto sua gravidez.

"Nós somos a fonte da cobiçada mercadoria; nossa experiência é objeto da extração." (SHOSHANA ZUBOFF, 2020, p.168). Para o capitalismo de vigilância todo usuário, consumidor, trabalhador é uma mina de dados a serem extraídos para reforçar os softwares de análise, que atuam com base no *machine learning* (os programas aprendem com os usuários como se adaptar melhor a estes com base nos mesmos dados que esses usuários geram ao utilizar o software, um ciclo fechado), para que os modelos preditivos sejam cada vez mais precisos em prever comportamentos e preferências da experiência humana. A utopia do capitalismo de vigilância é ver os indivíduos tal qual Neo no filme Matrix via a realidade, uma série de dados a serem analisados a fim de não haver espaço para a individualidade, a transformação do humano em números e padrões que seriam capazes de identificar com uma precisão milimétrica o que o usuário deseja antes mesmo deste o desejar e conectar esse desejo com uma empresa que seja consumidora deste mercado futuro. Nas palavras de Larry Page (CEO Google): "Na minha visão a longuíssimo prazo [...] nosso software entende a fundo tudo o que pode saber sobre você, o que não se pode saber e como organizar o mundo possa resolver problemas importantes." (SHOSHANA ZUBOFF, 2020, p.477).

Condensadamente, o *capitalismo de vigilância* consiste na datificação da experiência humana através dos dados que produzimos cada vez mais. As empresas buscam vender com precisão quais os nossos comportamentos futuros serão paras outras empresas a fim de que haja uma perfeita simbiose do desejo do usuário com a oferta da empresa, as empresas operantes no mercado futuro vendem a certeza de entregar o produto exatamente para aqueles que o desejam no momento exato que eles o desejarem, as custas dos nossos dados que são a matéria prima que move toda a roda desse novo modelo capitalista preditivo.

1.2. Matéria-prima; Dados

Em 2006 o matemático britânico Clive Humby afirmou “Data is the new Oil!” (Dados são o novo petróleo, tradução nossa) e não poderia ter sido mais preciso em sua constatação. Desde o berço da civilização moderna a sociedade vem produzindo cada vez mais dados, cabe aqui ressaltar que a não só a nossa visão moderna de dados é suficiente quando falamos em contexto histórico, desde que a civilização greco-romana (berço da civilização ocidental em que vivemos) começou o seu expansionismo iniciou-se a coleta dos dados produzidos pelo homem.

Censos populacionais, tamanhos de exércitos, número de nascimentos e mortes e afins foram sendo escritos e guardados pela civilização ocidental em detrimento da história oral de outrora, mais e mais criamos o hábito de registrar e arquivar acontecimentos meteorológicos, populacionais, espécies descobertas, tipos de medicamentos encontrados e inúmeras outros dados que a medida em origina-se a prensa de Gutemberg cada vez mais temos acesso a dados das populações ancestrais. Esse registro de todas essas informações fora usado por Malthus para criar suas teorias populacionais demográficas, por Karl Marx para desenvolver o seu modelo econômico socialista e por Adam Smith para criar a sua teoria liberalista de mercado, a famosa “mão invisível”, entre outros gigantes que usaram os dados para desenvolver teorias que revolucionaram a civilização moderna.

Entretanto os dados do mundo analógico, onde os dados eram arquivados em papéis e registros que ocupavam um espaço físico e requerem um espaço absurdo para seu armazenamento e um esforço hercúleo para sua consulta, não eram de acesso às massas, acessava os dados daqueles que iam às bibliotecas, arquivos públicos ou o governo e universidades que os usavam para seus objetivos uma vez que uma “pessoa comum” não teria como arquivar tanto volume de pastas e sequer ter o tempo para vasculha-las quando bem necessitasse. Portanto, com o advento dos computadores e das memórias digitais (disquete, pen drives, hard drives e cloud drives) tornou-se cada vez mais fácil a civilização armazenar e catalogar os dados, dando início ao chamado *Big Data*, que significa, resumidamente, o volume de dados gigantesco (maior de que um ser humano poderia ler em uma vida) armazenado nos computadores e drives do mundo inteiro.

O aumento exponencial de armazenamento dos dados graças ao advento dos drives digitais per si nada adiantaria, porém o ponto de inflexão que girou o capitalismo tradicional para o capitalismo vigilante é quando empresas como o Google percebem que podem transformar esse volume absurdo de dados em modelos preditivos, através do processamento e análise de Big Data armazenada os fundadores do Google criaram softwares (programas de computadores) capazes de analisar e processar os dados de forma que podiam determinar que

indivíduo estaria mais propenso a comprar um carro X e qual estaria mais propenso a comprar uma roupa Y.

Basicamente, o Google foi capaz de tirar vantagem desse volume de dados "morto" que estava sendo gerado para oferecer para as empresas "mercados futuros" onde eles entregam o produto que o cliente vai desejar para ele antes dele manifestar ativamente a sua vontade através da análise dos dados gerados por esse cliente, de forma ainda mais resumida, o Google tenta prever o que determinado usuário ira comprar com base na sua atividade de busca e navegação e entrega esse usuário a empresa que vende tal produto.

Os dados podem ser considerados o "novo petróleo" assim define o matemático Clive Humby, que ganhou popularidade a partir de um *report* da revista *The Economist de 2017*, intitulado "o recurso mais valioso do mundo não é mais petróleo, mas sim dados". Pois o petróleo sempre existiu, com seu potencial latente de energia, porém requer que haja o refinamento e mineração (análise e processamento) para que possa atingir o seu potencial de valor gerando riqueza para aqueles que o refina e entrega os produtos como gasolina, pneus e entre outros. Ainda nessa analogia, o Google se equipara a Standard Oil, empresa pioneira em refinamento de petróleo que dominou nos anos 60 como maior empresa do mundo, sendo pioneira e indisputada como quem descobriu como transformar os dados em uma matéria prima valiosíssima que transformou a economia global em uma economia "*data-driven*" onde a capacidade de análise e processamento de dados de uma empresa determina o qual bem-sucedida ela é.

Este novo mercado, "*data-based", "data-driven","data-guided*" e entre outros, é a própria manifestação do capitalismo de vigilância. Até empresas tidas como "tradicionais", que não vendem os dados dos seus clientes e sim bens de consumo, são hoje em dia totalmente focadas nos dados e em sua análise para definir estratégias e posicionamento.

Por exemplo, uma empresa do ramo cervejeiro perfila seus clientes, através de uma análise dos dados de compra ou sorteios, para saber onde posicionar seus produtos no supermercado gera maior venda, ou qual tipo de cerveja deve ser distribuída para diferentes zonas da mesma cidade a fim de maximizar os lucros. O uso dos dados tornou-se regra, e os cargos de analista de dados e processador de dados nunca foram tão valorizados quanto no capitalismo de vigilância.

1.3. A intimidade do indivíduo

Em uma sociedade cada vez mais instrumentalizada, onde os dados produzidos são o tempo todo coletados para processamento e análise, tal qual a nossa já se encontra, como o aumento do volume de processamento conjuntamente com a capacidade dos softwares de

gerar previsões precisas a respeito do nosso comportamento, é imperativo que observe-se os perigos evidentes e os não tão evidentes que nos aguardam nas próximas décadas.

> "Territórios íntimos do eu, como a personalidade e as emoções, são reclamados como comportamento observável e cobiçados por suas ricas reservas de superávit preditivo. Agora as fronteiras pessoais que abrigam a vida interior são oficialmente designadas como ruins para os negócios por uma nova espécie de mercenários do eu determinados a analisar e embrulhar a vida interior em nome das receitas da vigilância." (SHOSHANA ZUBOFF, 2020, p.349).

O íntimo individual do ser encontra-se em risco, o livre-arbítrio que é preconizado na Bíblia em sua alegoria do que nos difere de todos os outros seres e que nos torna humanos, a individualidade e auto afirmação individual estão sendo engolidas pelos ganhos econômicos que a coleta de dados proporciona. As *"big techs"* (grandes empresas de tecnologia que são as pioneiras do modelo capitalista discutido nesse tópico) realizam a coleta de dados ininterruptas através dos nossos computadores, smartphones, tablets e afins. Há um estado de constante vigilância, não à toa esta foi a palavra utilizada por Zuboff, do indivíduo já que quanto mais informações a precisão das previsões serão maiores, numa relação direta de proporcionalidade.

A intimidade é um conceito ultrapassado para os capitalistas de vigilância, apenas um obstáculo a ser suplantado a fim de que os *softwares* sejam capazes de conhecer o indivíduo na sua totalidade e prever todos seus possíveis comportamentos. O indivíduo deixa de pertencer a si mesmo, uma vez que sua persona vira um profile que pertencem as "*Big techs*", sendo um problema de duas sortes. A autora Ana Frazão, esclarece bem que a predição e os julgamentos feitos por decisões algorítmicas classificam, perfilizam e desconsideram a individualidade do ser humano, além de resultarem uma diferenciação de tratamento que pode marginalizar alguns indivíduos. Acerca dos resultados produzidos pelas decisões algorítmicas, a autora ressalta:

> "os algoritmos preocupam tanto quando acertam como quando erram. Preocupam quando acertam, pois, podem revelar aspectos íntimos de nossa personalidade que gostaríamos de manter em segredo, até porque podem ser utilizados para tolher o exercício de direitos e oportunidades. Preocupam quando erram, pois desconfiguram a nossa individualidade atribuindo-nos características que não temos e que também podem ser utilizadas para nos tolher direitos e oportunidades, com o agravante que tais decisões são baseadas em juízos totalmente equivocados" (FRAZÃO, 2019, p. 13).

Essa invasão ao terreno íntimo, à privacidade e ao indivíduo junto da completa renderização da experiência humana em números e dados analíticos a serem utilizados para dar a fim a nossa individualidade imperam que repense-nos o que entende-se por privacidade. Não deve-se ficar inerte perante aos avanços cada vez mais velozes na nossa vida íntima, ao santuário do privado, afinal foi estabelecido desde a modernidade que o indivíduo tem direito

a seu santuário privado, onde se retrai do público para se resguardar, a casa como santuário do indivíduo. Nas palavras do poeta Bachelard:

> "A casa abriga sonhos e devaneios, a casa protege o sonhador, a casa permite que se sonhe em paz [...]. É o primeiro mundo do ser humano. Antes de ser "jogado no mundo" [...] o homem é deitado no berço da casa." (Bachelard Gaston, A poética do espaço, São Paulo,2008, p.6.).

2. PRIVACIDADE

2.1 História da privacidade

Em 1988 a Constituição Federal não utilizou o termo "privacidade", mas sim deu a expressão de "intimidade" e "vida privada", dando a interpretação que a proteção da pessoa humana abrange ambos os aspectos. Há autores, como José Adércio Leite Sampaio, que creem haver diversidade nos dois termos e por isso analisa as particularidades de cada um.

> "Não obstante, julgarmos que, em princípio, a história do direito fundamental à intimidade e à vida privada será a história do homem em busca de realização de sua dignidade, será a história de suas lutas contra a opressão, o arbítrio, em prol da afirmação de sua liberdade, confundindo-se, nesse sentido, com a idealização e positivação dos direitos fundamentais." (SAMPAIO, p. 34).

Enquanto o autor Danilo Doneda, explana que a ausência de determinação terminológica na doutrina e jurisprudência pode ter sugerido o legislador a optar pelo excesso, até pelo temor de reduzir a aplicabilidade da norma. Ou seja, tanto a expressão "vida privada" quanto o termo "intimidade" pretendem o mesmo objetivo, qual seja: tutelar a pessoa humana de forma mais clara possível, considerando a complexidade das situações subjetivas existentes. (DONEDA, p. 109-113).

Sendo assim, o autor Danilo Doneda, cita a teoria dos círculos concêntricos de Hubman, advertindo que os termos "vida privada" e "intimidade" fazem menção específica a determinadas amplitudes do desenvolvimento da proteção da privacidade, apresentando maior importância em determinado contexto histórico. Num primeiro momento, visualiza-se a esfera da intimidade (ou do segredo), depois a esfera privada e, em torno delas, a esfera social, que abrangeria a vida pública, incluindo os direitos à imagem e à palavra, mais abrangente do que a intimidade e a privacidade. (DONEDA, 2006, p. 108). Então para se compreender a concepção atual de privacidade, faz-se necessária uma breve digressão histórica acerca da origem da privacidade.

Portanto, a privacidade se entende hoje como um direito fundamental é uma construção jurídica relativamente recente no qual sofreu varias transformações, desde o tradicional conceito elaborado por Warren e Brandeis como o "The right to Privacy" de 1890 publicado pela *Havard Law Review*, até a concepção atual, caracterizada pela liberdade de

autodeterminação informativa, isto é, a capacidade de controlar as informações pessoais pelo seu titular.

Neste artigo de Warren e Brandeis, os autores discorrem sobre o conceito moderno da privacidade do indivíduo perante aos seus pares e perante ao Estado, de forma extremamente sucinta é o direito de um indivíduo não ter sua intimidade exposta, ações e pensamentos, que estejam no âmbito da esfera pessoal de sua casa e de sua família, mantidos fora do âmbito do público. No artigo citado, os autores trabalham a ideia de que a privacidade seria uma extensão do direito à propriedade, no sentido de que as ações, imagens e pensamentos da vida privada seriam parte da propriedade do indivíduo e, portanto, fora do alcance do Estado ou da comunidade.

Antes de nos aprofundarmos no trabalho de Warren e Brandeis, vale a pena pontuar como era vista a privacidade antes desse trabalho paradigmático. Nas sociedades pré-históricas tribais, não havia o conceito do privado, os indivíduos viviam como uma tribo em que tudo era compartilhado e experiência do junto, à própria tribo era um organismo vivo que lidava com as decisões de forma conjunta. Nas tribos, todas as zonas eram compartilhadas, os indivíduos dormiam sob um mesmo teto (ocas, malocas e acampamentos comunitários), comiam juntos e até as relações sexuais eram no mesmo local do convívio coletivo, não havia privacidade, como podemos observar nas comunidades indígenas que mesmo atualmente perduram a tradição do seus ancestrais.

Adentrando na era clássica, período greco-romano, berço da civilização moderna ocidental, não havia debate sobre o privado. Os filósofos gregos consideravam a *polis* um organismo vivo e comunitário no qual todos tomavam decisões juntos e essa visão de que havia uma comunidade aberta que todos faziam parte como iguais não permitia espaço para o surgimento da privacidade. Para os gregos e romanos a vida intima dos Deuses era motivo de lendas e mitos, assim como a vida sexual deles, os banhos eram públicos assim como o sexo em publico também era algo normal, o mais próximo da privacidade que chegaram os romanos eram os famosos bailes de máscaras, onde o individuo tinha oportunidade de agir como quisesse sem ser reconhecido, porém esse era um episodio isolado numa vida essencialmente comunitária e voltada a *polis*. “Pense na Roma Antiga como um gigantesco acampamento” (ALBERTO ANGELA, *A Day in the Life of Ancient Rome*, Translated by Gregory Conti, Europa Editions, Incorporated, 2009).

Durante a idade média, a privacidade começa a ganhar seus primeiros ensaios do que virá a ser a privacidade moderna. Com a expansão da igreja católica como principal juiz da cultura e da moralidade em todos os reinos, começou a existir um movimento de

marginalização do sexo, as camas medievais começaram a ser construídas com uma cortina que a ˜isolava" do mundo, simbolicamente demonstrando que as relações sexuais passam a ser algo privado dentro do casamento, longe dos olhos da comunidade ou do Rei. Porém a figura do Rei (escolhido por Deus, uma deidade) e da Igreja ainda eram presente na vida de todos, ao Rei e a Igreja nada era segredo e não podia esconder-se coisa alguma, havendo apenas essa privacidade da vida sexual de um casal por ser um dos dogmas da Igreja católica que o sexo era um ato "pecaminoso" e, portanto, deveria ser feito á margem da sociedade.

Figura 1: quarto na idade media

Fonte: ARTISTATION

Com o avanço da sociedade, cada vez mais o individuo passou a buscar a privacidade, à medida que o rei e a igreja iam perdendo sua força e o indivíduo começa a ser considerado inviolável a ideia de privacidade se fortalece, culminando no marco citado do trabalho de Warren e Brandeis:

> "A intensidade e a complexidade da vida, decorrentes do avanço da civilização, tornaram necessário algum recuo do mundo, e o homem, sob a influência refinadora da cultura, tornou-se mais sensível à publicidade, de modo que a solidão e a privacidade tornaram-se mais essenciais para o indivíduo ; mas o empreendimento e a invenção modernos, por meio de invasões em sua privacidade, o sujeitaram a uma dor e angústia mental, muito maior do que poderia ser infligida por uma simples lesão corporal." (HARVARD LAW REVIEW, The Right To Privacy, 15 de dezembro de 1890).

Para os autores, o homem passa a ser um indivíduo vulnerável ao público e sua privacidade é a parte inviolável na qual ele se protege do social. Vale ressaltar que no período de publicação desse trabalho as máquinas fotográficas tinham recentemente sido inventadas juntamente dos tabloides (revistas que divulgavam "fofocas" sobre a vida sexual e intima de pessoas notórias) e cada vez mais debatia-se os limites das fotos e da exposição da vida pessoal do indivíduo.

Assim nasceu a privacidade moderna, baseada na jurisprudência de Thomas M. Cooley (Juiz da Suprema Corte the Michigan 1864 - 1885) que cunhou o termo *"Right to be left alone"*(Cooley on Torts, 2 ed., p. 29). Que indicava o direito do individuo de não ser importunado pelas novas tecnologias que ameaçavam a vida doméstica e intima á época.

2.2 Privacidade Moderna

Por muitos anos a ideia da privacidade construída em 1890 foi suficiente, com os devidos avanços na hermenêutica dos direitos individuais e as adições ao direito de autodeterminação, liberdade religiosas, direito a imagem e propriedade intelectual. Muitos foram às evoluções que corroboram o direito a privacidade, porém em seu núcleo permaneceu o mesmo do fim do século XIX, porém com o avanço do capitalismo de vigilância precisamos revisitar tais conceitos uma vez que estão ficando ultrapassados.

Não há como tratar da privacidade moderna sem citar o trabalho do professor Stefano Rodotá, civilista italiano que em seu trabalho "A vida na sociedade de vigilância" aprofunda-se na evolução necessária da privacidade do século XIX para a privacidade do século XXI. Para Rodotá, com a coleta de dados cada vez mais massiva a relação do indivíduo com a sua intimidade deixa de ser sigilosa, pois na sociedade moderna o sigilo é algo utópico, uma vez que estamos sendo monitorados initerruptamente através dos nossos aparelhos e tecnologias, e não há a opção de "*shut down"* (ficar completamente off-line) uma vez que a própria sociedade tornou-se hibrida (digital e analógica), se o individuo decide se desconectar ele imediatamente irá cair no ostracismo social voluntario.

Rodotá propõe uma nova opção ao sigilo, o controle; ao invés da sociedade buscar pelo sigilo de suas informações para resguardar a sua privacidade (utópico e impraticável) deve ser dado ao individuo o poder de controlar como serão usados seus dados a fim de resguardar seus melhores interesses, a proposta (a qual concordamos que seja a melhor saída) é a transição do "pessoa, informação, sigilo" para "pessoa, informação, circulação, controle, gestão". Resumidamente, Rodotá aceita que é impossível mantermos os sigilos dos nossos dados, e, portanto, busca empoderar o indivíduo para que este possa exercer o controle e gestão dos seus dados a fim de que não seja prejudicada sua privacidade.

A nova privacidade no século XXI não consiste no direito do indivíduo de ser deixado em paz, de ter suas preferências e desejos mantidos em sigilo da sociedade, a expansão do capitalismo de vigilância tornou impossível tal objetivo que era alcançável pela privacidade do século XIX. Na atualidade resta entendermos o ambiente em que vivemos de coleta massiva de dados e constante vigilância, aceitando que é impossível nos evadir de tal cenário e lutar pela busca do controle de como serão utilizados esses dados e pela transparência das

empresas para que nossa privacidade continue nas mãos e controlada pelo indivíduo, a nova privacidade é o controle sobre nossas informações ao invés do sigilo da primeira**.**

E no âmbito brasileiro, o Marco Civil da Internet (Lei n° 12.965) foi primeiro a estabelecer de forma direta os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Motivados pelas movimentações internacionais já mencionadas, os legisladores brasileiros sentiram a necessidade de compilar essas normas em um código específico, de forma a favorecer o acesso normativo a todos, criando assim a Lei Geral de Proteção de Dados.

Portanto o direito à privacidade no Brasil é previsto tanto na Constituição quanto na legislação infraconstitucional, pois é considerado direito fundamental e direito da personalidade, sendo uma figura jurídica que supera a dicotomia entre direito público e privado**.**

3. GDPR — GENERAL DATA PROTECTION REGULATION

General Data Protection Regulation (GDPR), é uma lei da Europa, que em português significa Regulamentação Geral de Proteção de Dados. Esta lei tem o objetivo de aumentar o rigor com a proteção de dados que envolvem as identidades de cidadãos europeus**,** e assim impactando diretamente as empresas que operem com plataforma online**.** Alguns exemplos são lojas virtuais, serviços financeiros, redes sociais, entre outros ambientes digitais que coletem e armazenem dados de seus visitantes e leads. E consigo traz dois principais conceitos que é a transparência e a responsabilidade, no qual nada pode ficar oculto para o titular dos dados e as empresas devem ter um cuidado maior para que os dados estejam em segurança.

A GDPR foi criada por causa dos grandes casos de vazamento de dados, a utilização e comércio de informações pessoais, a União Europeia decidiu revisitar suas regras de proteção de dados. E assim obrigou empresas de todo mundo, inclusive gigantes como o Facebook e o Google, a mudar a forma como coletam e tratam dados e foi responsável por uma nova onda de novas leis sobre o tema em todo o mundo, inclusive no Brasil.

Um dos maiores escândalo, por exemplo, foi o caso da *Cambridge Analytica*[4], em que chamou a atenção e indignação da mídia, do público, de parlamentares e reguladores em todo

[4] "A Cambridge Analytica é uma empresa de análise de dados que trabalhou com o time responsável para campanha do republicano Donald Trump nas eleições de 2016, nos Estados Unidos. (https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml).

o mundo, demonstrando que sim, as pessoas se preocupam com violações de sua privacidade e abuso de poder.

Em 17 de março de 2018, os jornais *The Guardian* e *The New York Times* publicaram simultaneamente histórias expondo como os dados pessoais de mais de 50 milhões de usuários do Facebook acabaram nas mãos da Cambridge Analytica, uma empresa que buscou aumentar o apoio à campanha presidencial de 2016 Donald Trump.

Cambridge Analytica era uma empresa de consultoria e análise de dados fundada pelo bilionário americano de direita Robert Mercer e chefiada pelo fundador da Breitbart Steve Bannon antes de partir para servir como executivo-chefe da campanha 2016 do Trump. Os relatórios cobriram como Cambridge Analytica usou dados para traçar o perfil e direcionar eleitores individuais com o objetivo de prever e influenciar suas decisões de voto. Relatórios revelaram ainda que Cambridge Analytica também apoiou a campanha Brexit no Reino Unido. Os dados coletados pela empresa incluíam detalhes sobre identidades dos usuários, rede de amigos e "curtidas". A ideia era mapear traços de personalidade baseados no que as pessoas gostavam no Facebook e usar as informações para segmentar públicos-alvo com anúncios digitais.

De acordo com os jornais, no final de 2015, o Facebook estava ciente de que Cambridge Analytica havia explorado os dados de seus usuários, mas o Facebook não informou as pessoas que foram afetadas e se envolveram em esforços limitados e ineficazes para recuperar seus dados. O Facebook mais tarde admitiu que o número de pessoas afetadas era muito maior do que haviam relatado inicialmente na verdade, ele compartilhou os dados de 87 milhões de usuários.

Com isso, houve a maior multa já aplicada a uma empresa por violação de dados pessoais. O Facebook foi autuado pela FEC – *Federal Trade Commission* a pagar algo em torno de R$ 25 bilhões de reais (US$ 5 bilhões de dólares), em 2019.

Este escândalo foi um dos muitos que ilustram que a privacidade também diz respeito à autonomia, dignidade e autodeterminação das pessoas e uma pré-condição necessária para a democracia.

Portanto, a GDPR foi o incentivo para o Brasil promulgar a Lei Geral de Proteção de Dados (LGPD) e também para o mundo, visto que a partir desta lei, outros países também visaram em proteger mais os dados pessoais da sociedade. Assim claramente influenciada pelos princípios da diretiva europeia, a LGPD foi criada com os principais pontos de dá direito para o titular acessar, editar ou solicitar a exclusão de seus dados, recolhimento autorizado

(com exceção em casos específicos), maior cuidado com dados sensíveis, portabilidade de dados e sanções administrativas se houver descumprimento.

Nesse sentido, o ponto principal que a LGPD busca propagar é a consciência de que os titulares dos dados são cidadãos, que possuem direitos e devem ser respeitados. Sendo assim, as empresas não podem fazer o que bem entendem com as informações dessas pessoas.

4. O DIREITO DA PRIVACIDADE NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD

O direito da Privacidade é profundamente ligado com a Lei Geral de Proteção de Dados Pessoais, pois a privacidade resguarda alguns direitos da pessoa, como a intimidade e o sigilo das telecomunicações, impedindo o Estado de intervir na vida privada, ou seja, o direito à privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito.

Já a Lei Geral de Proteção de Dados Pessoais, ao mesmo tempo em que reconhece a importância do tratamento de dados para desenvolvimento econômico e tecnológico, objetiva também em conferir instrumentos para que a pessoa tenha certo controle e autonomia em relação ao que é feito com seus dados, pois como já comentado no tópico anterior a LGPD surgiu em decorrência da tendência mundial em trazer maior transparência nos processos de manipulação de dados pessoais dos cidadãos. E a LGPD traz justamente a mudança na forma que é coletada as informações dos dados pessoais do individuo, buscando sempre a segurança da pessoa física, para que a honra e a imagem não seja denegrida.

O direito à privacidade e a LGPD promove a personalidade humana, o poder de escolha e decisões individuais, pois a possibilidade de autodeterminação é importante aspecto da própria dignidade humana. Como observa Jorge Reis Novais:

> "a titularidade de uma qualquer posição de direito fundamental envolve, em princípio, o poder de disposição sobre todas as possibilidades de ação que dela decorrem, momento o poder de disposição acerca do 'se', do 'quando' e do 'como' do seu exercício (ou não exercício) fático". (NOVAIS, JORGE REIS, 2006, p.286)

Por exemplo, no contexto de interfaces digitais, entende-se a coleta como a ação que o site ou sistema executa para a captura dos dados pessoais de alguém, seja através de um formulário, tela de cadastro em um aplicativo ou mesmo processamento de identificadores eletrônicos como *cookie*s e IP, mas para isso o art.6°, inciso I da LGPD explana alguns princípios que devem ser respeitados, como a necessidade e a finalidade que precisa ser clara, de modo que o usuário possa identificar, com clareza e sem palavras difíceis ou escondidas, qual será a finalidade que a empresa dará àquele dado uma vez informado pelo usuário, ou

seja, a coleta deve ser claramente transparente em suas ações, mostrando o propósito conhecido e informado, e não subentendido ou meramente genérico para armazenamento e uso futuro. Sendo assim, coletar dados em excesso ou para prever futuras campanhas de publicidade, segmentação e compartilhamento com terceiros, não é mais permitido (não que fosse "permitido" antes), sendo essa uma mudança vasta para sites e sistemas que dependem de grande volume de dados pessoais e que sempre foram acostumados a "coletar o máximo que puder" para "quando precisar".

O art.5°, inciso I da Lei Geral de Proteção de Dados Pessoais, esclarece que os dados são quaisquer conjuntos de informações que possam levar a identificação de uma pessoa natural, de maneira direta ou indireta (identificada ou identificável), por referência a um nome, a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social, ou seja, não são apenas dados diretos que identifiquem uma pessoa, mas sim, um conjunto de dados que podem vir a potencialmente identificar uma pessoa.

E evidenciando especificamente o direto à imagem, no artigo 2º, inciso IV da Lei nº 13.709 da LGPD, dispõe que a proteção de dados pessoais tem como fundamentos a inviolabilidade da intimidade, da honra e da imagem, ou seja, está lei elevou o direito à imagem ao nível máximo de proteção pelo novo sistema, fazendo com que tenha um cuidado mais rigoroso com a segurança da imagem do individuo.

Além disso, no art. 5º, inciso II da LGPD enfatiza sobre os dados pessoais sensíveis que recebe um tratamento específico, e um deles é o dado genético ou biométrico, e que é classificado dentro do direito á imagem, logo dentro dos dados biométricos existe varias espécie que faz a identificação, como o reconhecimento da face, de voz, de digitação, de assinatura, impressão digitais, o estilo da escrita e entre outro também, mas é importante salientar que isso já foi detalhado através do Decreto 10.046/2019 no art. 2º, II, que dispõe que os dados biométricos são “características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar”. E isso mostra o quanto é invasiva a obtenção dos dados sensíveis, o que justifica o tratamento mais rigoroso, pois a falta transparência e conhecimento de como os dados pessoais são coletados e utilizados, podem levar a consequências não assistidas que violam os direitos individuais e coletivos.

Por isso é necessário que as empresas e principalmente os aplicativos das redes sociais estejam regulamentados com a norma da LGPD, visto que os termos de privacidade e

segurança dos aplicativos deverão ser mais objetivos e concisos sobre a finalidade daquela coleta de dados. Mesmo se o aplicativo for estrangeiro, todo dado coletado em território brasileiro estará sujeito à LGPD brasileira.

E para isso, as coletas de dados pessoais só poderão ser apuradas quando houver recomendações quanto à finalidade, e a temporalidade com o consentimento do indivíduo, por se tratar de dados pessoais sensíveis o tratamento gera riscos às liberdades civis e aos direitos fundamentais e por isso deve ser solicitado o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), de modo que no art.38º, da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, dispõe que a ANPD (Autoridade Nacional de Proteção de Dados) poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente as suas operações de tratamento de dados, observados os segredos comercial e industrial. Ainda, a referida autoridade poderá solicitar ao controlador a elaboração do RIPD, quando o tratamento for realizado com base em seu legítimo interesse, de acordo com o artigo 10, § 3º, LGPD:

> "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. "

Bem como para os agentes do Poder Público, com base no artigo 32° da LGPD:

> "Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público. "

No entanto, é importante questionar a base legal que irá justificar esse tipo de tratamento, uma vez que não é possível obter o consentimento de toda e qualquer pessoa que poderá ter suas informações coletadas. No caso de não haver o tratamento de dados sensíveis, a empresa poderá optar pelo legítimo interesse, assim exposto no art. 7°, inciso IX, X da LGPD:

> "7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
> "

Visto que, é de total interesse da empresa garantir a segurança de seus empregados e de suas dependências para optar pela garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, no caso em

que houver o tratamento de dados pessoais sensíveis. Conforme disposto no Art. 11°, II, g da LGPD:

> "Art. 11°. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. "

Ou seja, não é possível postar qualquer imagem sem autorização das pessoas retratadas nesses casos de exceção de aplicação da LGPD, uma vez que continua em vigor o direito de imagem. Nesses casos, permanece importante analisar se houve consentimento ainda que tácito das pessoas, ou se a foto ou o vídeo foram produzidos em espaço público, se há interesse público na divulgação da imagem, dentre outros pontos tradicionalmente discutidos quanto a esse direito da personalidade.

Percebe-se que o direito à privacidade protege os dados pessoais pertinentes ao seu detentor, o qual possui discricionariedade em mantê-los sob seu domínio ou, se preferir, expô-los, podendo impor limites e condições, observando os ditames do ordenamento jurídico a que se submete.

5. O DIREITO DE FICAR *OFF-LINE*

5.1 Ficar 100% *off-line*

A cada ano que passa a palavra "*off-line*" fica mais distante da sociedade, pois a tecnologia revolucionou o mundo, porque ela está em tudo, e suas alterações são visíveis e invisíveis. Novas empresas foram criadas através da tecnologia, por exemplo, os bancos digitais, e as empresas físicas tiveram que migrar para a internet, pois não há um palco maior do quê a internet para o oferecimento dos seus produtos. Além disso, hoje em dia vivemos em uma sociedade que as intimações judiciais podem ser feita por Whatsapp.

A internet, inquestionavelmente, traz uma melhoria substancial nas condições de acesso aos serviços jurisdicionais, em que todos possam reivindicar os seus direitos mais básicos. Trazendo um ambiente virtual mais democrático, auxiliando diretamente no aperfeiçoamento da imagem estrutural do Judiciário, ao buscar encurtar as desigualdades sociais.

A Lei de Informatização do Processo Judicial (lei 11.419/06) autoriza o uso de meio eletrônico na "tramitação de processos judiciais, comunicação de atos e transmissão de peças

processuais" (art. 1º) e o aplicativo WhatsApp se enquadra ao conceito jurídico de "meio eletrônico" previsto em lei no art. 246° do CPC e na Lei 11.419/06, art.1°,§ 2º, II.

> **"Art. 246**. A citação será feita preferencialmente por meio eletrônico, no prazo de até 2 (dois) dias úteis, contado da decisão que a determinar, por meio dos endereços eletrônicos indicados pelo citando no banco de dados do Poder Judiciário, conforme regulamento do Conselho Nacional de Justiça. (Redação dada pela Lei nº 14.195, de 2021).
>
> **Art. 1°**- O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.
> **§ 2° -** Para o disposto nesta Lei, considera-se:
> **II** - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;"

Um bom exemplo foi o pedido concedido pelo o desembargador Rômulo Russo, da 7ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo, em que autorizou a citação da parte contrária que reside no exterior para que fosse feita pelo WhatsApp, em uma ação de alimentos, em razão da pandemia da Covid-19.

Na decisão, o desembargador ressalta que a citação pela via virtual, por meio do aplicativo, é providência que se sintoniza com a legalidade escrita do art. 246° do CPC e PCA do CNJ:

> "Além disso, é ferramenta indispensável à agilidade e à entrega da prestação jurisdicional dentro de prazo razoável, mormente em citação a ser efetivada em outro país, com a consabida lentidão, agora carregada por força da pandemia que a todos assola."

Dessa forma, considerou possível o provimento do agravo para a citação por via virtual, "sendo certo que o dano de difícil reparação é inerente à hipótese, sobretudo em demanda que versa direito de família".

A pesquisadora LEVINE (2014, p. 56), em seu estudo sobre a tecnologia, observou que "a confiança e a cooperação são aspectos críticos do funcionamento da sociedade, e o foco da sociedade contemporânea está mudando para a comunicação digital e a interação".

Portanto, não tem como ficar *off-line*, nosso mundo já migrou pro digital, é preciso, adaptar-se a essa nova realidade, pois se o indivíduo escolhe ficar *off-line*, o mesmo acaba sendo prejudicado, visto que essa pessoa será limitada em suas ações. Assim também entende também a pesquisadora Shoshana Zuboff (2020, p. 285): "os clientes podem optar por participar ou não do compartilhamento de dados. De outro lado, aqueles que se recusam a ser incluídos se defrontam com uma finalidade limitada do produto e de segurança de dados."

5.2 Alternativas para o controle da coleta de dados

Ao invés de tentar se desconectar, as pessoas podem controlar a forma que se dá a essa conexão, saber para onde vão os dados, de que forma está sendo utilizado, e claro pedir a transparência no uso de informações pessoais, de modo que a LGPD concede ao titular todos esses direitos, assim previsto em Lei:

> "Art. 9º. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei."

Assim também como consta no regimento da GDPR, determinando que as organizações que processam e controlam dados de pessoas residentes da União Europeia só poderão ser utilizados com o consentimento do mesmo. Além disso, o consentimento deverá ser pedido de forma inteligível, facilmente acessível, usando linguagem clara e simples. A coleta dados pessoais devem ser tratados de forma lícita e transparente, garantindo a lealdade com o titular, também deve haver finalidades específicas para o tratamento dos dados.

Assim, o usuário é o real proprietário de seus dados pessoais e terá o direito de ter o conhecimento sobre as informações por ele concedidas ao controlador dos dados, quais dados estão sendo processados, quem está processando as informações e qual finalidade.

O usuário também tem o direito de realizar a portabilidade dos dados de uma controladora para outra, ou até mesmo ter um "backup" dos seus dados. O direito ao esquecimento também é um ponto importante da GDPR, uma vez que o usuário terá o direito de solicitar ao controlador que apague seus dados pessoais e interrompa a disseminação dos mesmos.

Portanto, é vidente que tanto a LGPD como a GDPR tem diversos pontos similares, fazendo com que ambas tenha o suporte necessário para garantir o direito da sociedade no mundo da tecnologia. Além disso, mostra que a coleta já virou o padrão, pois o mundo gira em torno de coleta de dados, não tem como retroceder, por isso foram criadas para que tanto a pessoa física como a jurídica sejam asseguradas pela Lei.

Por exemplo, um caso recente do TRT da 2° Região de São Paulo, em que um funcionário em seu trabalho encaminhou para seu e-mail particular uma planilha contendo dados pessoais de terceiros de outros funcionários e clientes que eram protegidos tanto pelo

regimento interno da empresa com pela LGPD, aos quais teve acesso em razão da atividade desenvolvida na empresa, e por descumprimento das políticas internas da companhia, foi demitido por justa causa e o Tribunal confirmou a demissão com relação ao amparo à proteção da Lei Geral de Proteção de Dados, de acordo com o processo (nº 1000612-09.2020.5.02.0043). Essa decisão reforça a aplicação da norma, que tem como principal objetivo proteger os dados dos usuários.

Portanto é importante salientar que a melhor alternativa para as coletas de dados é controlar a forma que é coletada os dados, pois o indivíduo que optar em ficar *off-line*, o mesmo acaba sendo prejudicado, visto que essa pessoa será limitada em suas ações.

6. ANÔNIMIZAÇÃO DOS DADOS

Outra alternativa que a Lei Geral de Proteção de dados trás é a anonimização dos dados do titula em que consiste na utilização de meios técnicos que um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Segundo a LGPD, a anonimização é uma referência técnica que garante a segurança de dados pessoais. O dado anonimizado é definido como aquele relativo a titular que não possa ser identificado, tendo em vista a utilização de "meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Art. 5º, III, LGPD). E a técnica de anonimização é definida como a "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*"* (Art. 5º, XI). Ou seja, sua finalidade é garantir a privacidade de uma pessoa ou empresa, preservando a credibilidade dos dados coletados e eventualmente repassados.

Existe um tratamento de exceção ao dado anonimizado na LGPD, especificamente no art. 12°, onde dispõe "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, […]". Isso significa que uma vez que o dado é anonimizado, a LGPD não será aplicada, pois não é possível identificar ou associar a um dado real o dado anonimizado.

Diferente dos dados pseudonimizados que a LGPD prevê, nos termos do parágrafo 4º do art. 13º. De acordo com esse artigo, tal procedimento consiste em anonimizar dados, mas com a possibilidade de reversão do processo, desde que seja controlada pelo detentor em ambiente seguro, que ainda mantém possibilidades de identificação e continuam sujeitos à lei:

> "Art. 13. §4º. Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".

Ou seja, a pseudonimização contribui para garantir uma maior segurança dos dados, podendo diminuir os danos causados por eventuais vazamentos, se os dados afetados forem

somente aqueles não identificáveis, sem o acesso aos dados complementares mantidos em separado. Este cenário pode fazer com que eventuais indenizações sejam reduzidas ou mesmo não aplicáveis, considerando que os dados vazados não sejam capazes de gerar danos ao titular por serem incompreensíveis.

Na continuação da redação do art. 12°, é mencionado que "salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido." Nesta hipótese de excepcionalidade à frase inicial do artigo, a reversão do dado anonimizado ficará sujeita às técnicas de anonimização aplicadas para efetuar a proteção e reaproveitamento dos dados.

Já no parágrafo 1º deste mesmo artigo há a determinação de que custo e tempo necessários para reverter o processo de anonimização devem ser considerados de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. No parágrafo 3º do art.12º, a ANPD poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Outro ponto importante em salientar, é que no art. 16°, inciso II e IV, prevê a conservação dos dados após o término do seu tratamento para finalidades de estudo por órgão de pesquisa e para uso exclusivo do controlador.

> "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

Observa-se que a anonimização é utilizada como forma de legitimação, seja para autorizar um tratamento, seja para autorizar armazenamento mesmo após o término de um tratamento.

A vista disso, essa é uma das técnicas que empresas podem usar para cumprir regulamentos de privacidade de dados que exigem a segurança da informação. É o caso, por exemplo, de dados de identificação pessoal como relatórios de saúde, informações de contato e detalhes financeiros. E é essencial que as empresas também ofereçam segurança no sentido de blindar dados para impedir tipos de ação ilegais, como os dos hackers.

Dessa forma, respeitar os limites legais relativos à anonimização de dados garante que uma empresa esteja dentro da lei. Assim, ela não só assegura a privacidade dos usuários de seus sites e redes sociais como o enquadramento legal, evitando penalidades. E ao garantir o

anonimato às pessoas que navegam em seus sites, uma empresa se posiciona ao lado do seu maior patrimônio, o cliente. Então, respeitar as regras de anonimização não é só uma questão de respeito às leis como também um assunto estratégico e de interesse comercial.

Por fim, sobre a anonimização, é essencial olhar para o que entende o autor Azambuja (2019, p. 26-27).:

> "Vários modelos de anonimização que podem ser utilizados para preservar a privacidade dos usuários são propostos na literatura. O avanço tecnológico não garante uma eficaz segurança da informação, sem uma conscientização do ser humano em relação à segurança. O acesso não autorizado a informações, lugares, objetos, entre outros tipos de dados, na organização, torna a segurança vulnerável, uma vez que as pessoas e as empresas interessadas nesses dados têm acesso indevido a essas informações. As políticas de privacidade dos serviços on-line oferecidos pelas organizações devem estar em conformidade com a LGDP e GDPR. As referidas leis podem aplicar penalidades para as organizações que não se prepararem corretamente para a coleta, a gestão e o uso dos dados privados dos usuários. Estar *compliance* com a LGDP e GDPR será não só uma oportunidade para melhorar e aumentar o nível de privacidade, segurança e gerenciamento de dados, como um diferencial para os novos modelos de negócio baseados em dados. Em 2018, emerge o conceito de que somos o produto do espaço cibernético. Grande quantidade de informação é publicada no ciberespaço e os sistemas que recebem esses dados ficam cada vez mais inteligentes, ou seja, são capazes de fazer cruzamentos que nem imaginamos."

Portanto, fica evidente que a LGPD oferece um grande incentivo para o uso de dados anonimizados, apesar de nem todas as formas de tratamento poderem se utilizar de tal categoria de dado.

7. CONSIDERAÇÕES FINAIS

O avanço da capacidade de processar e analisar dados forneceu o cenário ideal para empresas como a pioneira Google desenvolverem os seus sistemas e modelos preditivos que deram a partida do novo modelo capitalista vigente, o capitalismo de vigilância. Tal modelo refina e explora a matéria prima mais abundante e inesgotável que existe no momento; dados.

A exploração dos dados através de *softwares* cada vez mais inteligentes gerou um verdadeiro frenesi onde todas as companhias começaram a buscar cada vez mais formas de acessar e minerar os dados dos seus usuários para fins econômicos.

Essa exploração desgovernada só teve precedentes históricos na exploração dos combustíveis fósseis no começo da primeira revolução industrial, e tal momento provocou danos ecológicos que repercutem sem remédio que geram consequências nefastas até os dias presentes, por isso devemos estar alertas ás possíveis consequências que tal mineração de dados podem afetar nossas gerações atuais e futuras.

Principalmente, a nossa privacidade tal qual a concebemos resta impactada por esse novo modelo capitalista. A privacidade, que consiste num espaço do intimo do individuo de

ter suas informações guardadas em sigilo aquiesceu pois com a sociedade hibrida (digital e analógica) não mais temos a opção de manter nossas informações em sigilo, as empresas coletam em tal grau nossos dados que a opção de estar off-line tornou-se ilusória. Devemos evoluir para uma sociedade que a privacidade é o potencial de controlar e gerir os dados que nos são coletados, empoderando o individuo para que ele possuo o direito de auto determinação digital.

Portanto, o empoderamento da relação indivíduo x coletor de dados deve avançar com base em uma nova visão hermenêutica da privacidade e utilizando-se da LGDP como marco normativo que visa proteger e garantir o direito a nova privacidade. A LGPD nos preconiza que o individuo tem o direito de saber como, onde e quando seus dados são utilizados a qualquer momento, tendo o direito de correção dos dados, sendo esta lei o instrumento a ser utilizado para buscarmos a promoção da autonomia dos indivíduos no controle dos seus dados e na defesa dos seus direitos perante as grandes empresas que mineram nossos dados para ganho econômico.

Finalmente, a era em que podíamos escolher ser anônimos e manter nossa vida intima em total sigilo findou. Não existe cenário em que uma pessoa possa escolher ficar off-line sem resultar num auto ostracismo da vida em sociedade. Portanto, deve-se buscar evoluir o debate sob a ótica da nova privacidade, utilizando da LGPD como ferramenta fundamental na defesa da anterior a fim de garantir o controle e a autonomia do individuo em relação aos seus dados.

REFERÊNCIAS

ANGELA, Alberto. **A Day in the Life of Ancient Rome**. Editora: Europa, 2009.

AZAMBUJA, Antonio João Gonçalves. **A privacidade, a segurança da informação e a proteção de dados no Big Data**. Brasília-DF. 2019. Disponível em: http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/914/831. Acesso em: 15 nov. 2021.

BRASIL. Presidência da República. **Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Redação dada pela Lei nº 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 out. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 1. ed. em e-book baseada na 2. ed impressa. ed. São Paulo: Thompson Reuters, 2019. Disponível em: https://proview.thomsonreuters.com/title.html?redirect=. Acesso em: 20 out. 2021.

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

FTC. **A FTC impõe multa de US $ 5 bilhões e novas restrições de privacidade abrangentes no Facebook.** 2019. Disponível em: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions. Acesso em: 01 nov. 2021.

GATEFY**. Principais pontos de comparação entre a LGPD brasileira e a GDPR europeia. 2021.** Blog Educação. Disponível em**:** https://gatefy.com/pt-br/blog/pontos-comparacao-lgpd-brasileira-gdpr-europeia/#:~:text=A%20LGPD%20brasileira%20(Lei%20Geral,parte%20de%20empresas%20e%20organiza%C3%A7%C3%B5es.&text=%C3%89%20uma%20lei%20que%20abrange,e%20foi%20implementada%20em%202018. Acesso em: 01 nov. 2021.

GDPR. E. **O que é o GDPR, a nova lei de proteção de dados da UE?.** Disponível em: https://gdpr.eu/what-is-gdpr/. Acesso em: 01 nov. 2021.

HILL, K. **Como o alvo descobriu que uma adolescente estava grávida antes do pai.** 2012. Revista Forbes. Disponível em: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=484e88a06668. Acesso em: 25 out. 2021.

Figura 1. Quarto na Idade Média. **Artstation**. Disponível em: https://www.artstation.com/artwork/XBK63y. Acesso em: 25 out. 2021.

NOVAIS, Jorge Reis. **Perspectivas constitucionais: nos 20 anos da Constituição de 1976**. Coimbra: Coimbra Editora. 1996.

OPICE, Renato. Blum. **Proteção de Dados. Desafios e Soluções na Adequação à Lei.** Ed. Forense. 2020.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje: Parte I(Tecnologia e Direitos)**. Renovar, 2008.

RODOTÀ, Stefano. **El derecho a tener derechos. Madrid: Editorial Trotta**, 2014. ISBN 978-84-9879-538-7.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1998.

TEPEDINO, G; FRAZÃO A; OLIVA, M. D. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 1ª ed. São Paulo. Thomson Reuters Brasil, 2019. Disponível em: https://forumturbo.org/wp-content/uploads/wpforo/attachments/45774/4042-LGPD-e-Suas-Repercusses-no-Direito-Brasileiro-Gustavo-Tepedino-2019.pdf. Acesso em: 11 nov. 2021.

THE ECONOMIST. **O recurso mais valioso do mundo não é mais petróleo, mas dados**. 6 de maio de 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 10 nov. 2021.

WARREN, S; Brandeis, Louis. **(December15,1890). "The Right to Privacy"**. IV. ED. Harvard Law Review Retrieved 4 June 2021 – via Internet Archive.

ZOBUFF, Shoshana. **A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder**. 1ª ed. INTRÍNSECA, 2020.

.

AGRADECIMENTOS

Eu Arthur, quero agradecer ao meu Pai, minha namorada e minha amiga Letícia que me ajudaram nessa caminhada. E não menos importante, a mim mesmo, que sempre superei todas as expectativas.

Eu Neila, primeiramente gostaria de agradecer a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida, e não somente nestes anos como universitária, mas que em todos os momentos me guardou, e me deu força para superar todas as dificuldades.

Agradeço aos meus pais Nelio e Jouse, por serem a minha maior base, pois sempre estiveram ao meu lado me apoiando, fazendo de tudo pra que eu realizasse esse grande sonho, aqui fica minha imensa gratidão, por sempre terem sonhado junto comigo e nunca ter deixado eu desistir, vocês são minha maior inspiração.

Sou grata a minha família Cunha e Oliveira, pelo grande apoio que me deram durante essa caminhada, sem eles eu não teria conseguido chegar até aqui. Obrigada Tias/tios que me incentivaram a crescer e por me acolher durante esses cinco anos em suas casas, aqui fica gratidão, amo muito cada um de vocês. Não poderia também deixar de mencionar minhas primas/primos, que sempre estiveram comigo mesmo estando longe, mas eles sempre me apoiaram.

Quero agradecer também aos meus amigos, por todas as palavras de incentivo para não desistir deste sonho. Posso dizer que Deus me enviou muitos anjos pra estar comigo durante toda essa caminhada, aqui fica minha imensa gratidão a todos vocês.

Essa conquista não é só minha, é NOSSA!