UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS
GRADUAÇÃO EM DIREITO

LUIZMAR PEIXOTO DANTAS

A SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Cidade de Goiás
2022

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): LUIZMAR PEIXOTO DANTAS

Título do trabalho: A SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Bruna Pinotti Garcia Oliveira**, **Professora do Magistério Superior**, em 20/04/2022, às 11:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **LUIZMAR PEIXOTO DANTAS**, **Discente**, em 20/04/2022, às 12:16, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site

https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2846972** e o código CRC **1987ED0C**.

Referência: Processo nº 23070.017432/2022-45 SEI nº 2846972

LUIZMAR PEIXOTO DANTAS

A SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Trabalho de Conclusão de Curso de Graduação – TCCG, requisito para aprovação na disciplina Monografia Jurídica II, do Curso de Direito da Unidade Acadêmica Especial de Ciências Sociais Aplicadas do Campus Goiás da Universidade Federal de Goiás – UFG, e para obtenção do título de Bacharela em Direito.

Orientador:
Profa. Dra. Bruna Pinotti Garcia.

Cidade de Goiás
2022

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Dantas, Luizmar Peixoto
A SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) [manuscrito] / Luizmar Peixoto Dantas. - 2022.
LIV, 54 f.

Orientador: Profa. Dra. Bruna Pinotti Garcia.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Direito, Cidade de Goiás, 2022.

1. Autodeterminação Informacional. 2. Dados Pessoais. 3. LGPD. 4. Segurança da Informação. 5. Direito à privacidade. I. Garcia, Bruna Pinotti, orient. II. Título.

CDU 34

UFG

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos 12 dias do mês de abril do ano de 2.022 iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado "A SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)", de autoria de LUIZMAR PEIXOTO DANTAS, do curso de Direito da Unidade Acadêmica Especial de Ciências Sociais Aplicadas da UFG. Os trabalhos foram instalados pela Presidenta Prof. Dra. Bruna Pinotti Garcia Oliveira – orientadora (UAECSA/UFG) com a participação dos demais membros da Banca Examinadora: Prof. Dra. Sofia Alves Valle Ornelas (UAECSA/UFG) e Margareth Pereira Arbués (UAECSA/UFG). Após a apresentação, a banca examinadora realizou a arguição do estudante. Posteriormente, de forma reservada, a Banca Examinadora deliberou e considerou o TCC aprovado.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Bruna Pinotti Garcia Oliveira**, **Professora do Magistério Superior**, em 20/04/2022, às 11:55, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Margareth Pereira Arbués**, **Professor do Magistério Superior**, em 20/04/2022, às 12:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Sofia Alves Valle Ornelas**, **Professora do Magistério Superior**, em 21/04/2022, às 15:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2846923** e o código CRC **12CEDD00**.

Referência: Processo nº 23070.017432/2022-45 SEI nº 2846923

Exaltação de Aninha

A estrada da vida é uma reta marcada de encruzilhadas.
Caminhos certos e errados, encontros e desencontros
do começo ao fim.
Feliz aquele que transfere o que sabe e aprende o que ensina.
O saber se aprende com mestres e livros.
A Sabedoria, com o corriqueiro, com a vida e com os humildes.
O que importa na vida não é o ponto de partida, mas a caminhada.
Caminhando e semeando, sempre se terá o que colher.

Cora Coralina.

AGRADECIMENTOS

Ninguém é tão alguém que não precise de ninguém. É seguindo essa filosofia de vida que agradeço primeiramente a Deus por capacitar as pessoas que estão ao meu lado para ter condições de me ajudar e apoiar em tempos tão difíceis. Dentre eles, minha mãe Maria Aparecida Peixoto Dantas, e meu pai Luiz Evangelista Dantas. Pessoas que dão o melhor de si para que eu possa dar o melhor de mim.

Família é benção de Deus, somente com ele temos força pra seguir em frente. Cabe citar minha irmã Marina Peixoto Dantas, minha tia Maria Evangelista Dantas, minha avó Benedita Peixoto, meu avô Estandeslau Evangelista, minha tia Deni Moreira Marçal, minhas primas Natalia Moreira Marçal e Fernanda Moreira Marçal, meu primo Luan Oliveiral Marçal, e meu tio Waldomiro.

Ademais, existem pessoas que encontramos pelo caminho e fazem valer a pena toda a caminhada. Dentre elas, minha companheira Isabela Aparecida Azevedo Coqueiro e a Eliane Azevedo. Através de vocês aprendi o significado de graça.

Aos amigos que levo pra vida, mesmo que indiretamente ajudaram de alguma forma, João Paulo Oliveira Cabral, Gustavo Sarafim do Carmo, Caio Cesar da Silva, Katryel Alcântara, Luiz Henrique Borges.

Ao ensino público gratuito e de qualidade, personalizado na figura dos professores, técnico e servidores. Em especial a Bruna Pinotti Garcia Oliveira que tenho grande admiração, e ao João Paulo Lopes Machado que através das atitudes me ensinou como ser um grande gestor.

Para o que serviria a ciência senão para satisfazer os anseios da sociedade. Por isso, é muito importante que as pesquisas visem não somente o meio acadêmico, mas principalmente o viés social. Tudo aqui é para honra e gloria de Deus, assim como pelo bem do próximo, principalmente aos que carecem de informação, aos que estão em situação de vulnerabilidade e aos que tem seus direitos violados.

Por fim, trago a seguinte citação: “Os rios não bebem sua própria água; as árvores não comem seus próprios frutos. O sol não brilha para si mesmo; e as flores não espalham sua fragrância para si. Viver para os outros é uma regra da natureza. (...) A vida é boa quando você está feliz; mas a vida é muito melhor quando os outros estão felizes por sua causa”. Papa Francisco.

RESUMO

A revolução informática e tecnológica juntamente com a popularização dos dispositivos eletrônicos mudou a realidade e o cotidiano da sociedade. O arranjo social tornou-se centrado nos dados, tornando-se esse o componente central para promoção da economia e das relações de poder. Nesse contexto, aflorou-se uma busca incessante e massificada por dados, em que o proprietário de tais dados possui condição de vulnerabilidade, levando em conta a relação assimétrica que impede sua autodeterminação informacional. Existe então, a necessidade de nos alertarmos para um cenário de potencial lesividade aos direitos fundamentais, podendo o uso indevido dos dados, afetar diretamente tanto na vida privada do usuário (vazamento de dados bancários) quanto na sociedade em geral (influenciando nas eleições). Vários mecanismos legislativos foram editados para regular tal situação, mas o grande divisor de águas veio em 2018 com a LGPD, pois ela representa o consentimento, isto é, o dever de solicitar a autorização do titular dos dados, antes da coleta e do tratamento a ser realizado (físico ou digital), sendo executado de forma explícita e inequívoca. Entretanto, a lei por si só não impede que as violações continuem acontecendo, isso porque, os violadores utilizam dos mais diversos artifícios para coagir ou ludibriar os cidadãos para que forneçam seus dados. Nessa seara, esta pesquisa propõe, através de pesquisa exploratória, descritiva e qualitativa de cunho bibliográfico, doutrinário, jurisprudencial e documental, a evidenciar o valor dos dados pessoais na atualidade, demonstrar a importância da autodeterminação informacional e seus desafios, e dissertar como a LGPD e a segurança da informação podem ser usadas como ferramentas práticas de proteção contra ataques aos direitos à privacidade de dados.

Palavras-chave: Dados Pessoais; LGPD; Segurança da Informação; Direito à privacidade.

ABSTRACT

The computer and technological revolution together with the popularization of electronic devices has changed the reality and daily life of society. The social arrangement became data-centric, making this the central component for promoting the economy and power relations. In this context, an incessant and mass search for data emerged, in which the owner of such data has a condition of vulnerability, taking into account the asymmetric relationship that prevents their informational self-determination. Therefore, there is a need to alert ourselves to a scenario of potential harm to fundamental rights, and the misuse of data can directly affect both the user's private life (leakage of bank data) and society in general (influencing elections). Several legislative mechanisms were enacted to regulate this situation, but the great watershed came in 2018 with the LGPD, as it represents consent, that is, the duty to request the authorization of the data subject, before the collection and treatment to be carried out. be performed (physical or digital), being performed explicitly and unequivocally. However, the law alone does not prevent violations from continuing to happen, because violators use the most diverse artifices to coerce or deceive citizens into providing their data. In this area, this research proposes, through exploratory, descriptive and qualitative research of a bibliographic, doctrinal, jurisprudential and documentary nature, to highlight the value of personal data today, demonstrate the importance of informational self-determination and its challenges, and discuss how the LGPD and information security can be used as practical tools to protect against attacks on data privacy rights.

Key words: Personal data; GDPR; Information security; Right to privacy.

SUMÁRIO

INTRODUÇÃO

Alberto da Silva é professor de história no ensino médio e pretende viajar para ministrar aula em determinada escola da cidade vizinha. No dia seguinte, pela manhã, o chuveiro já está ligado e as torradas estão quase prontas, esperando por Alberto. Todos os aparelhos da casa estão cronometrados com o horário da viagem. Inclusive, a sua geladeira, que já encomendou leite e ovos ao supermercado, para quando Alberto retornar de viagem.

Durante o café da manhã, Alberto se desequilibra e deixa café cair no chão, mas não precisa limpar pois seu robô que faz faxinas doméstica já está programado para limpar assim que Alberto sair de casa. Pouco mais de 05 (cinco) minutos, o motorista de aplicativo já está buzinando em frente à sua porta devido o horário que já estava programado na agenda. O motorista já tem a rota da escola e toca a playlist de músicas favoritas de Alberto.

Ao chegar, é só descer do carro, o pagamento já foi realizado via cartão de crédito. Ele se dirige, então, diretamente ao portão de entrada e percebe que esqueceu o crachá de professor, mas não tem problema porque tem reconhecimento facial para acesso à escola.

Depois de encerrar a aula que ministrou em voz alta sobre cultura japonesa, sentiu fome e abriu o celular em busca de restaurantes. Logo de cara são sugeridas, pelo site de busca, várias promoções de sushi e sashimi localizados próxima a ele. Apesar de nunca ter experimentado tais pratos, Alberto decidiu conhecer. Ao chegar no local, foi recepcionado por atendentes que logo solicitaram seu nome, e-mail, e telefone dizendo que faz parte do procedimento de reserva da mesa no estabelecimento.

Após se alimentar, decide pedir a conta e o caixa do estabelecimento pergunta se quer CPF na nota. Alberto diz que não, mas o atendente insiste dizendo que oferece desconto. Por fim, com intuito de evitar delongas, Alberto oferece seu CPF e paga a conta com seu Smartwatch, tendo em vista que esqueceu sua carteira em casa. Ao sair na porta do restaurante, o motorista de aplicativo já te espera para o retorno à sua casa depois do dia de trabalho.

Esse exemplo fictício foi adaptado da obra do Ricardo Bioni “Proteção de dados pessoais: a função e os limites do consentimento”, mas não está longe de nossa realidade. É valido ressaltar que todas automações citadas no exemplo só aconteceram devido Alberto ter aceitado os termos das políticas de privacidade em cada aplicativo e empresa correspondente.

É perceptível que com todas essas automações, nosso cotidiano fica mais conveniente e confortável. Todavia, para que tudo isso possa acontecer, temos que abrir mão da privacidade de certos dados pessoais.

Nesse sentido, sobrevém o seguinte questionamento: até que ponto essa automação vale a pena em detrimento do direito à privacidade?

É com base nesse questionamento que essa pesquisa toma raízes. Isso pois, a sociedade é reféns dos meios digitais, no sentido que atualmente tudo em nosso cotidiano tem relação com a tecnologia. O mercado toma medidas agressivas para adquirir a posse dos nossos dados a qualquer custo. Muitas das vezes o consentimento dado pelo usuário, mesmo que autônomo não é valido. Isso porque, além das técnicas utilizadas pelas empresas, também existe a limitação cognitiva, informacional e econômica do indivíduo, que influenciam para que esse consentimento não seja válido.

A primeira parte deste trabalho consiste em fazer um breve histórico dos dados pessoais, desde o surgimento da internet, até os dias atuais. A denominada sociedade informacional surge exatamente nesse cenário de busca constante por informações. Nesse contexto, os dados alcançam status de grande valia, com isso surge a necessidade de proteção. Diversas leis foram editadas nesse sentido, perpassando por três gerações. Até chegar no estágio atual com a LGPD, o brasil não possuía regulamentações especificas visando a proteção dos dados, nesse sentido, as discussões nesse trabalho terão como ponto de partida a promulgação da LGPD.

A partir dessas colocações, passa-se à segunda parte da pesquisa em que destaco a importância da autodeterminação informacional e os desafios para que o consentimento seja atingido de maneira válida e eficaz. Pontuações sobre as consequências da não proteção dos dados são necessárias para demonstrar a importância da proteção. Superado isso, é preciso perceber que existem diversos obstáculos que impedem com que a autodeterminação informacional seja atingida de maneira plena. Dentre elas temos as limitações cognitiva, estrutural e econômica do usuário, além das técnicas antiéticas utilizadas pelo mercado visando driblar a legislação e capturar os dados a qualquer custo, a exemplo da disseminação de discursos limitantes e do desenvolver de trakers.

Por fim, a terceira parte trata dos meios de proteção dos dados pessoais através da LGPD e da segurança da informação. Somente a repressão legislativa não é suficiente, até porque a tecnologia está em constate modificação e o direito não tem plenas condições de estarem sempre alinhados com tal demanda, até por conta da burocracia legislativa. Assim sendo, tem-se que a melhor forma de se defender é entender seus inimigos, dessa maneira, este trabalho elenca as técnicas utilizadas pelo mercado informacional para de obtenção dos dados dos usuários. Logo, a segurança da informação com banes nos regramentos estabelecido pela LGPD, traz métodos para proteção dos dados pessoais, que vão desde a utilização de antivírus até o gerenciamento das câmeras e microfones dos nossos aparelhos eletrônicos.

Portanto, infere-se que é fundamental perceber a importância da autodeterminação informacional nos dias atuais para não ter direitos fundamentais violados e o não sofrer as consequências de ter seus dados vazados. Mesmo com a proteção legislativa que busca o consentimento, existem limitações que impedem que o consentimento seja válido. Nesse sentido, deve-se buscar meios para que haja o empoderamento do indivíduo, através de, não somente alterações legislativas, mas também conhecimento da segurança da informação. Só assim será possível, capacitar e emancipar o indivíduo em meio a economia informacional.

CAPÍTULO 1 – VALOR DOS DADOS PESSOAIS

1.1 Contexto Histórico

O contexto histórico, em grande parte dos desenvolvimentos de teses, pesquisas e estudos é de extrema importância para ambientar e contextualizar o leitor acerca do tema proposto.

Ao tratar da temática acerca dos dados pessoais, bem como sua evolução histórica é inevitável falar-se em internet e como essa se desenvolveu ao longo do caminhar da sociedade. Isso ocorre porque o termo e conteúdo "dados pessoais" já existia antes da internet, mas ganha grande visibilidade e valor quando a revolução tecnológica torna esse elemento uma espécie de tesouro, como já foi o carvão mineral na revolução industrial, o petróleo no século XX e atualmente os dados pessoais no século XXI.

Nesse contexto, a internet foi o instrumento principal para que os dados pessoais emergissem como o grande tesouro do século XXI, e isso dá-se ao momento dramático ocorrido entre os anos de 1947 e 1991 no contexto da Guerra Fria, entrave entre as duas grandes potências mundiais da época: Estados Unidos da América e União Soviética.

A Guerra Fria, repartiu o planeta em dois grandes polos cada uma liderado pelos dois grandes países da época. Concerne em um conflito político e ideológico o qual provocou uma corrida de produção tecnológica, bélica e intelectual entre os países, resultando em algumas ações bélicas espalhadas pelo mundo, como a Guerra da Coreia (1950 e 1953), Guerra do Vietnã (1959 e 1975), Guerra do Afeganistão (1979). Apesar de todos esses conflitos, o maior momento de tensão foi o episódio conhecido por "Crise dos Mísseis em Cuba" ocorrido em 1962, momento em que Cuba após passar por uma revolução nacionalista em 1959 se aliou a União Soviética a qual instalou uma base de misseis no país que tem a localização geográfica extremamente próxima dos Estados Unidos, representando o maior momento de tensão.

Nesse cenário, emerge a necessidade de transmitir os dados de uma forma rápida e eficaz, resistente a limitações territoriais ou físicas que não encontraria empecilhos para percorrer enormes distancias e chegar com rapidez ao local de destino. Como muito bem menciona Abreu, no final da década de 50 e início dos anos 60 por meio da produção bélica e para fim militares os estadunidenses veem a utilidade de um complexo que otimizava o tráfego de informações e com isso foi iniciado os projetos para o surgimento da internet (ABREU, 2009).

Dessa forma, foi criado um sistema de conexão de computadores em bases militares estadunidenses sendo que o primeiro sistema foi chamado de Advanced Research Projects

Agency – ARPA (Agência de Investigação de Projetos Avançados) e nasceu em 1958. Logo em seguida, em 1962 a Agência de Investigação de Projetos avançados, inovou criando uma programação chamada Arfante com o fim de interligar as bases militares e os departamentos de pesquisa do Estado Americano, tal fenômeno foi visto como o elemento inicial para o desenvolvimento da internet (FORTES, 2016).

Posteriormente, em 1970 os primeiros testes entre a sociedade civil ocorreram nos Estados Unidos. Os experimentos ocorreram no âmbito universitário enviando dados de uma universidade para outra sendo que ao final trinta e oito universidades americanas já transmitiam dados pela internet, sendo que a rede Arpanet passou a atender tanto o ambiente universitário como também as bases militares.

Nesse apanhado de acontecimentos, após os testes realizados entre as Universidades americanas, entendeu-se que o uso da tecnologia poderia avançar muito além do que vinha sendo usado. Dessa forma, em 1978 foi criado uma espécie de modem de máquina por estudantes universitário de Chicago-EUA sendo que tal dispositivo, tornou possível as transferências de programas atrás da linha telefônica e posteriormente passam a surgir os primeiros provedores de serviços online nos Estados Unidos e Europa.

É fundamental salientar que no início do desenvolvimento tecnológico a internet era de difícil acesso, até mesmo pelo ambiente no qual ela surgiu, exposto acima. Essa realidade começa a mudar na década de 90. Segundo Abreu (2009, p. 27):

> Em meados de 1990, o Centro No Centro Europeu de Pesquisas Nucleares - CERN, localizado em Genebra na Suíça, cria o World Wide Web - WWW, por um grupo de pesquisadores liderados por Tim Berners-Lee e Robert Cailliau, que **introduziram a ideia de integração de computadores mundialmente, tal elemento contribuiu totalmente para tornar a internet um meio de comunicação de massa.**

Como menciona Fortes (2016, p. 52):

> A World Wide Web foi uma ferramenta preponderante pela disseminação da internet não apenas entre os indivíduos de determinadas sociedades, mas também entre os países, sendo que com tal alastramento e fácil acessibilidade a internet se tornou um meio de comunicação em massa bem como o maior meio de compartilhamento de dados e informações

1.2 Sociedade Informacional

Ao passar dos anos, a sociedade passou por diversos modelos estruturais de organização social. Nesse contexto, um elemento estrutural central, sempre existiu e estabeleceu os respectivos marcos históricos de suas respectivas épocas.

Em sociedades rurais, as riquezas advinham do campo. Com os avanços tecnológicos, vieram criações como as máquinas a vapor e a energia elétrica. Em especial com o fim da Segunda Guerra Mundial, houve grande destaque para o departamento de serviços, que adquiriram função de grande destaque no cenário econômico da época.

A era pós industrial teve como característica uma sociedade que não era mais identificada pelo que seria capaz de fabricar, mas sim pelos serviços que poderiam ser por ela ofertados. No atual estágio, a sociedade está enraizada pela forma organizacional que tem por núcleo os dados, tai qual substitui os recursos que anteriormente estruturava as sociedades previamente citadas.

Nesse interim, o novo modelo de organização social foi alavancado pela recente evolução tecnológica, que criou novos dispositivos com capacidade de transmissão de dados, nunca antes visto. Até a forma de conviver socialmente foi afetada pelo fluxo informacional de forma que não existem mais barreiras físicas de distância.

No mesmo sentido como foi a terra, o motor a vapor, máquinas, eletricidade e os serviços, nas sociedades rurais, industrial e pós-industrial, respectivamente, os dados tornou-se o novo elemento estruturante que reorganizou a sociedade moderna.

Nesse interim, é possível compreender que as sociedades pós-industriais possuem economias fortemente baseadas em tecnologias e tratam informações e dados como seus principais produtos. Assim sendo, os grandes valores produzidos nessa economia não são originários da indústria ou de bens físico, mas sim da produção de bens virtuais, os quais podem ser transmitidos no meio cibernético nesse sentido Sergio Amadeu (2017, p. 21) afirma:

> O sistema capitalista promovia a fluidez do capital e o aumento de sua circulação no espaço-tempo mundial. O capital como mercadoria na esfera da circulação precisava diminuir o tempo da conversão em dinheiro e o tempo de retorno ao capitalista para ser reempregado na sua ampliação.

Na atualidade, pós-industrial, os dados a respeito do consumo da mercadoria retornam aos CEO’s da empresa como ferramenta principal da busca pela reprodução do capital. Dados como: a maneira de consumo do produto, o lapso temporal da compra e os metadados da

transação. Dessa forma, a medida com que as vendas vão acontecendo, mais dados dos perfis dos compradores são arrecadados.

Cabe ressaltar, que o rápido crescimento das redes digitais criou importantes mudanças nas formas de propriedade e de venda de produtos com enfoque na indústria cultural, na música, notícias, nas mídias sociais, na literatura e no audiovisual. Diferente do mercado pré-industrial, no mercado financeiro, as redes cibernéticas proporcionaram grandes avanços/modernização das contínuas tentativas de gerar retorno financeiro sem o desgaste da produção.

Empresas do mercado informacional incorporaram essas tecnologias cibernéticas facilmente. A revolução tecnológica também reduziu o custo de logística e trabalhistas das operações, o que proporcionou grande aumento no lucro das empresas. Nesse mesmo contexto, de forma progressiva as empresas financeiras passaram a substituir trabalhadores físicos por máquinas, sensores e softwares.

As novas tecnologias da informacionais, satisfaz os especuladores que buscam estratégias diferentes para captar o fluxo do mercado, como também para propagar informações que possam modificar o comportamento dos compradores. Portanto, quando se trata das sociedades informacionais a principal caraterística é ter seus mecanismos comandados e organizados por meio virtual, através das maquinas. Segundo Lev Manovich (2013, p. 52):

> "sociedade informacional", "sociedade do conhecimento" ou "sociedade em rede" são denominações para sociedades dependentes de software. Os softwares, atualmente, não só organizam a internet, seu roteamento e os sistemas de compartilhamento de informações, mas também estão presentes em escolas, hospitais, sistemas sociais e tributários, bem como na gestão das cidades, aeroportos, hidroelétricas e usinas nucleares.

A coletividade informacional, produz vários registros em larga escala. Determinadas decorrências sociais, econômicas e políticas possuem a necessidade de ser melhor compreendidas.

Conforme o portal Statista publicado no ano de 2017, em seu último relatório, constatou que ao final de 2017 o planeta continha um número de aproximadamente 3,58 bilhões de internautas. O fato é que tal número tende a continuar se alargando tendo em vista a forma como os meios eletrônicos têm se popularizado na sociedade.

Ademais, o Instituto Brasileiro de Geografia e Estatística – IBGE no ano de 2016, estima que no Brasil há 116 milhões de pessoas com acesso à rede, que resulta em 64,7% dos brasileiros. Todavia, é importante considerar que diante da sistemática atual, grande maioria desses brasileiros pertencem a classe média alta e ricos, sendo que as classes menos favorecidas

ainda não têm essa amplitude de acesso.

Em um panorama geral, quatro são os fatores preponderante para que a internet alcance o mundo todo: a facilidade (pode ser acessado pela maioria dos dispositivos hoje); a relevância (o intuito do usuário ao se conectar); acessibilidade (baixo custo de acesso); Disponibilidade (exige pouco investimento em infraestrutura). Tudo isso implica em uma rede globalizada que quebra barreiras físicas e dissemina acesso a todas as culturas.

Por conseguinte, as inovações trazidas pela internet trouxeram inúmeras transformações sociais e econômicas o que possibilita, nas palavras de Araújo (2017, p.62): “Afirmarmos que hoje vive-se em uma Era Digital, momento no qual a maioria das coisas e atividades humanas podem ser realizadas por meio da internet, tratando-se assim de uma realidade virtual que funciona concomitantemente com o mundo real”.

Logo, a internet não se restringe mais apenas a computadores, como no início de seu desenvolvimento, estando na verdade permeada por vários outros dispositivos usados no dia a dia das pessoas, como notebooks, computadores, tablets e celulares, utensílios que dia após dia ajudam no desenvolvimento da qualidade de vida humana.

Assim, em um mundo cada vez mais tecnológico, nasce a inteligência artificial (IA) criada com a intenção de fornecer mais facilidade a rotina humana, proporcionando mais conforto, comodidade e segurança ao usuário dos elementos tecnológicos. Os complexos algorítmicos assumem um papel de enorme importância e aceleram o crescimento da economia em razão da rapidez de processamento das informações.

Desse modo o grande ponto positivo da IA é a drástica diminuição dos erros e a capacidade de alcançar uma enorme precisão na execução de atividades. Ademais, deve ser ressaltado que a inteligência artificial tem a capacidade de processar vários dados recebidos por usuários e uma flexibilidade indispensável para aprender e de adaptar aos modos, gostos e gestos dos indivíduos. Com todos esses atributos é fácil perceber atualmente que a IA tem a capacidade de substituir com facilidade a mão de obra humana por tecnologia, sendo perfeitamente possível que ela mesma desenvolva certas atividades. Isso pode ser observado pelas máquinas que executam montagem de carros, nas plantações de alimentos pelo maquinário agrícola entre outros.

Outrossim, deve ser ressaltado que a inteligência artificial para obter maior êxito está interligada com a Internet das Coisas (OIT). Refere-se a uma ligação, assim como a do cérebro e corpo humano, na qual a OIT, é um meio pelo qual os objetos físicos se conectam e falam entre si e se relacionam com os utilizadores através de softwares e sensores inteligentes que enviam dados para uma rede, criando um sistema de nervos que dá a possibilidade de trocar

informações entre dois ou mais elementos. Exemplificando, temos os eletrodomésticos, relógios inteligentes que contam calorias, passos, batimentos entre outros.

Dentro desse maquinário, a inteligência artificial transforma e processa a informações recebidas da OIT em dados utilizáveis e essa combinação que se torna cada vez mais avançada potencializada o poder tecnológico transformando-o em um elemento cada vez mais eficaz e capacitado para executar lições por meio do cruzamento de dados pessoais dos usuários.

Assim sendo, atualmente é viável afirmar que vivemos a Sociedade Informacional, pois desenvolveu-se um mundo digital que funciona paralelamente ao mundo real. Tudo isso devido as transformações relacionadas a evolução tecnológica e a internet. Com a rápida transmissão de dados, criou-se formas de interação social em que indivíduos, empresas, organizações e o Estado recebem e enviam informações de maneira quase instantânea, transpondo as barreiras espaciais, quebrando paradigmas e trazendo mais comodidade para o usuário.

1.3 Dados pessoais no século XXI

Como apresentado anteriormente, devido a revolução informática e tecnológica juntamente com a popularização dos dispositivos eletrônicos, hoje temos rápido e fácil acesso a qualquer tipo de informação na palma das nossas mãos, somos altamente interconectados, resolvemos problemas de maneira mais rápida e a inovação é imprevisível e espontânea.

Independente do lugar, seja na corrida matinal, vendo TV ou até mesmo parada no trânsito, virtualmente estamos sendo monitorados, e essa atividade cria um rastro digital, desde os relógios aos carros, tudo que se conecta na internet se torna dados.

Foi nessa conjuntura que os dados pessoais obtiveram maior relevância e alcançaram lugar de destaque, chegando a ser considerado o recurso mais valioso do mundo, desbancando o petróleo, segundo a Comissária Europeia para a Defesa dos Consumidores, Meglena Kuneva.

Em consequência disso, com o aumento do consumo das novas tecnologias, aumenta-se também a quantidade de dados captados. Isso pois, a coleta dados pessoais muda a natureza da concorrência, quanto mais usuários utilizam a plataforma, mais atraente fica para outras pessoas se cadastrarem. Assim ao arrecadar mais dados uma multinacional por exemplo tem um escopo mais amplo para aprimorar seus produtos o que atrai mais clientes gerando uma espécie de efeito cascata.

Nesse sentido, pode-se afirmar que a maior riqueza se encontra não nos dados propriamente ditos, mas sim na capacidade de usá-los de forma analítica. Essas informações precisam ser identificadas, catalogados, tratados, organizados e assim transformados em dados

em dados úteis.

Os responsáveis para que essas informações brutas coletadas em grande escala adquiram maior valor, são os algoritmos. Isso porque, após o processamento e tratamento dos dados, descobertas capazes de transformar a realidade não só das organizações, mas de diferentes mercados, podem ser extraídas. Sem esse tratamento, os dados, desconexos, não possui nenhum valor.

Não só no acesso à internet, como também no uso qualquer aparelho eletrônico ligados à internet, desde a geladeira à televisão, todos com uma capacidade crescente de coletar os dados dos seus usuários sob o pretexto de oferecer um serviço melhor, mais personalizado e prático. (THE ECONOMIST, 2017)

O controle desses dados pelas grandes potências da internet, tais como Google, Amazon, Apple, Facebook e Microsoft lhes dão imenso poder. Devido a coleta massificada de dados como: perfil de consumo, preferencias, círculo social, rotina, sentimentos, localização, interesses, contatos etc. Segundo Bioni (2021, p. 11), "aumentam-se as possibilidades de êxito junto a audiência, seja melhorando a concepção e a segmentação de um produto ou serviço, no que seja pertinente à abordagem publicitária para promovê-los".

Com essas informações a empresa pode melhorar seus produtos, atraindo então mais usuários, e por consequência, gerando ainda mais dados. Assim como também, através do marketing, pode ganhar mais assertividade para oferecer seus produtos de modo específico para o consumidor que tem mais possibilidade de os adquirir.

As redes sociais se destacam como plataformas de coleta desses dados, o que se dá geralmente por meio de testes, elaborados de forma atraente aos usuários, e que por meio do "aceite" do sujeito têm acesso a diversos dados como nome, idade, e-mail, e todas as fotos contidas no perfil do usuário (MENDONÇA, 2018).

A contra partida desses algoritmos é que os indivíduos podem ficar presos dentro de um filtro bolha, consumindo conteúdos que se encaixa nos seu respectivo perfil na plataforma. Além de dificultar uma visão sobre o que está fora desse círculo, os algoritmos geram uma comodidade tremenda aos indivíduos com uma temática de matéria cada vez mais especializado, que está nos separando ainda mais em grupos que não dialogam, tornando a sociedade cada vez mais polarizada.

Assim sendo, se por um lado as informações coletadas são utilizadas para proporcionar mais conforto e uma melhor experiencia para o usuário, por outro, serve também como instrumento para obtenção de lucro, através da ciência mercadológica, seja para transmitir um anúncio, vender um produto, ou até para alienar um ideal.

Outrossim, cabe ressaltar que na sociedade informacional, a coleta/análise de dados se dissemina por todos os indivíduos, independente de classe, raça, cultura, orientação sexual e etc. As empresas organizam possíveis estruturas de captação e de fidelização dos usuários. Para tanto, reúnem e fazem a análise dos dados dos usuários através de seus rastros digitais, ou seja, em seu uso diário das mídias e conteúdos virtuais. Dessa forma:

> Dados sobre nossa rotina de trabalho, estudo, entretenimento, são a formula base para a modulação de padrões e perfis de comportamento e de consumo. Tais informações trazem previsibilidade e facilitam a modulação do usuário. Esse é um dos motivos que tornou o mercado de dados pessoais de extrema importância para a economia informacional. (AMADEU, 2017, p.71).

De acordo com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a coleta desses dados, são a fonte principais de renda de grandes empresas como Google, Facebook, Twitter, Tiktok etc. Segundo eles:

> **O valor de empresas como o Facebook pode expressar o valor dos registros de dados pessoais em sua posse. Como exemplo, de 2006 a 2012, os dados dos usuários do Facebook oscilaram entre 40 e 300 dólares. Em maio de 2012 seu valor foi de 112 dólares por usuário**. Tais flutuações no valor do Facebook podem expressar não apenas a oscilações dos dados pessoais, mas podem ser produto de outros fatores econômicos. A publicidade com base no tratamento dos dados pessoais dos usuários é a grande fonte de receita do Google, em 2019, a publicidade superou 90% da receita total da empresa. (OCDE, 2020).

Percebe-se então, que mercado de dados pessoais que antes não obtinha tantos holofotes, ganha destaque com a ampliação das tecnologias digitais. Dessa maneira, entender sua dinamicidade e suas consequências se tornou tarefa inadiável. Nesse contexto, o Relatório da OCDE de 2013, alegou:

> A forma mais prática de obter o valor dos dados pessoais é aferir os preços de mercado em que são ofertados e comercializados. Os preços nos Estados Unidos para os dados pessoais variaram de 0,50 centavos para um endereço, 2 dólares para uma data de nascimento, 8 dólares para um número de seguro social, de 3 dólares para o número da carteira de motorista e 35 dólares para um registro militar. (OCDE, 2013, p. 255).

Através da economia de dados pessoais, o capitalismo informacional encontra uma favorável rentabilidade. Nesse sentido, informações acerca dos costumes de consumo, transações econômicas, círculo social, geolocalização dos cidadãos, permitem interpretar de

forma mais eficaz o mercado. Com isso, expande as probabilidades de sucesso, seja potencializando a qualidade um produto ou serviço, seja nos mecanismos de marketing e publicidade.

Todavia, a informação bruta não é o que impulsiona a produtividade no mercado informacional, mas sim o resultado do processamento e tratamento desses dados. Com o intuito de torná-la proveitoso e eficiente para a operação empresarial, os dados devem ser transformados em conhecimento. Nesta seara, os dados pessoais passam a ditar o ritmo de acumulo de capital na sociedade da informação.

1.4 Necessidade de regulamentação

Conforme a evolução da partilha de dados foi evoluindo, o direito também se modificou para acompanhar e preservar o direito à intimidade das informações individuais. Desse modo os países passaram a se movimentarem a fim de criar legislações capazes de regular esse tráfego tecnológico bem como proteger os direitos fundamentais das pessoas que muito mais passavam a fazer parte desse novo universo.

Com a constituição do Estado Moderno surge a carência de regulamentação em prol da guarda dos dados pessoais. Pós Segunda Guerra, os poderes administrativos dos Estados percebem que os dados pessoais dos seus cidadãos são proveitosos para arquitetar e organizar as suas ações.

Esse novo ângulo de vista do Estado somente foi possível graças às novas tecnologias, em especial a inteligência artificial que modernizou de forma quantitativa e qualitativa a aptidão de tratamento dessas informações.

A primeira geração de leis voltadas para proteção dos dados pessoais surgiu da preocupação que a coleta massiva dos dados pessoais dos cidadãos trazia para o Estado Moderno. Inicialmente, o recurso legislativo utilizado foi concentrar esforços na própria tecnologia que deveria ser domesticada e orientada pelos princípios governamentais do novo Estado Moderno.

Existia o receio do surgimento da figura Orwelliana do Grande Irmão, que segundo sua obra “1984”: “Na sociedade, todas as pessoas estão sob constante vigilância das autoridades, principalmente por teletelas (do original ‘telescreen’), a inversão dos valores – de proteção e zelo para controle absoluto; da assistência a alguém desprotegido para um comando tirânico”. (ORWELL, 2009, p. 40).

Ou seja, receio de haver a restrição da liberdade do indivíduo por uma vigilância ostensiva do Estado. Preferiu-se, ao contrário, criar mecanismos para controlar tais bancos de dados através da necessidade de permissão para o seu procedimento.

A primeira geração ficou marcada pelo acumulo de competências no âmbito governamental, assim como pelo pressuposto de estabelecer leis rígidas que monitorassem o uso da tecnologia. Todavia, a coleta e tratamento de dados ultrapassou o âmbito governamental, uma vez que aumentou a quantidade de agentes e bancos de dados a serem regularizados, nessa nova perspectiva fez-se necessário ampliar os campos normativos.

Na segunda geração, a principal característica é a mudança do núcleo regulatório. A preocupação não é mais exclusivamente as bases de dados do Estado, mas, também, com as do âmbito privado. Assim conforme Ricardo Bioni (2021, p. 109):

> Ao em vez de ter um banco de dados único e centralizado, é criado pequenos bancos de dados dispersos no plano estatal e privado. Assim, percebe-se que seria inviável a estrutura regulatória anterior em que era função do Estado licenciar a criação e o funcionamento dos bancos de dados. A segunda geração de leis confere ao próprio indivíduo a responsabilidade de proteger seus dados pessoais. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio usuário a gerência de seus dados que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais.

Outrossim ainda conforme o autor “o divisor de águas para a terceira geração de leis foi a amplitude do protagonismo do indivíduo na proteção dos dados pessoais” (BIONI, 2021, p.109). Desse modo nessa geração, as regras de proteção de informações individuais caminharam com o fim de se buscaram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento.

Assim “o objetivo seria que dessa forma alcançaria, o sucesso da própria terminologia da “autodeterminação informacional”, pois, com essa participação, possibilitaria que o sujeito tivesse um controle mais extensivo sobre as suas informações pessoais” (BIONI, 2021, p.109).

Ademais Bioni (2021, p.110) ainda afirma que:

> A disseminação de autoridades independentes para a aplicação das leis de proteção de dados pessoais, bem como de proposições normativas, que não deixavam ao indivíduo a possibilidade de escolha sobre o processamento de certos tipos de dados pessoais, relativizam os princípios de consentimento. A quarta geração veio para cobrir essa deficiência das gerações de leis anteriores. Contudo, esse progresso de gerações não acabou com o protagonismo do consentimento. O foco no consentimento permaneceu sendo a principal característica da abordagem regulatória. Tanto que, em meio a esse

> processo o evolutivo, o consentimento passou a ser qualificado, como devendo ser livre, informado, inequívoco, explícito e/ou específico, tal como no direito comunitário europeu. Essa distribuição de qualificadores acaba, portanto, por estabelecer um movimento em torno do papel de destaque do consentimento quase como sendo sinônimo de autodeterminação informacional.

Desta feita conforme o autor o progresso geracional normativo da proteção dos dados pessoais cria um processo no qual o consentimento emerge, é questionado e se reafirma como sendo o seu princípio central (BIONI, 2021, p.110).

1.4.1 Lei Geral de Proteção de Dados (LGPD)

A privacidade no Brasil e no mundo é um direito que vem sendo cada vez mais fortalecido, diante de inúmeras denúncias de utilizações de informações pessoais de forma abusiva, invasiva e indevida, sem mesmo que o titular tivesse qualquer controle sobre elas, havendo, inclusive, a sua utilização para fins políticos, econômicos ou sociais.

No ordenamento jurídico brasileiro, sempre existiu a preocupação acerca da proteção de dados pessoais, como por exemplo o próprio CDC (Lei nº 8.078/1990), a MCI (Lei nº 12.965/2014), a Lei de Acesso à Informação (Lei n° 12.527/2011), entre outras. Todavia, a impressão que passava era de uma "colcha de retalhos" devido nenhuma delas tratar especificamente dos dados pessoais e sua cadeia de consequências.

Dessa necessidade nasceu a Lei Geral de Proteção de Dados: uma lei brasileira, baseada na regulamentação Europeia (GDPR). A LGPD visa um equilíbrio entre o direito à privacidade e o uso massivo das informações pessoais. Sua missão, portanto, não é outra, senão proteger direitos fundamentais, tais como a liberdade, a privacidade, o livre desenvolvimento e a personalidade.

Como fundamentos da LGPD podemos destacar o respeito à privacidade, liberdade de expressão, inviolabilidade da intimidade, livre iniciativa, defesa do consumidor, direitos humanos, dignidade e exercício da cidadania.

Na prática, a LGPD se aplica aos governos e às empresas, tendo que garantir maior segurança aos dados pessoais, sempre observando a finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, responsabilização e a prestação de contas de tudo que se refere aos dados pessoais, conforme bem explicado durante o presente trabalho.

De forma geral, a LGPD é uma regra para todos, ou seja, cria um cenário de segurança

jurídica válido para todo o país; estabelece de maneira clara, o que são os dados pessoais e como deverá ser feito o devido tratamento deles. Como regra, para que os dados pessoais possam ser tratados, deve haver o consentimento do seu titular, tendo como exceção apenas os casos em que seja indispensável cumprir critérios legais.

Nesse contexto, conforme explica Dhiulia Santos (2019, p.67):

> Ao analisar a LGPD, é possível constatar que em relação ao **consentimento do usuário**, tal tópico tem essencial direção no que tange a esta legislação e a seus efeitos, pois, enquanto no Marco Civil da Internet, tal palavra consta somente 3 (três) vezes, ao longo da **nova lei pode-se notar cerca de 35 (trinta e cinco) vezes**, algo que revela uma abordagem mais significativa do tema, bem em como os legisladores se preocuparam em sua regulação.

Mesmo assim, é importante notar que, apesar de a lei dar aos usuários a opção de escolher como seus dados são usados, não há garantia de que esse direito será respeitado, razão pela qual o consentimento pode enfrentar dificuldades no cumprimento das obrigações estabelecidas na legislação.

Dhiulia Santos (2019, p. 13) afirma ainda que:

> Um outro desafio quanto ao consentimento do usuário como instrumento legítimo ao tratamento de dados pessoais, é o fato de que este procedimento, por vezes aparenta-se como inócuo, haja vista que os seus efeitos deste tratamento não são tão nítidos ao titular dos dados pessoais. Ademais, em estudo realizado por pesquisadoras americanas, estima-se que os usuários dispenderiam, pelos menos 201 horas por ano se procedessem à leitura de todos os termos de uso dos websites que são em média acessados por um usuário americano.

Portanto, é preciso reconhecer que a mera aceitação do consentimento de um titular de dados pessoais para o controle de suas informações é insuficiente para preservar um direito fundamental à proteção de dados. Com isso, a Lei nº 13.709 estabelece um conjunto de princípios que nortearão o tratamento de dados de forma que, se seguidos, resguardarão os direitos fundamentais dos usuários em relação ao objeto deste estudo.

CAPÍTULO 2 – A IMPORTÂNCIA DA AUTODETERMINAÇÃO INFORMACIONAL E SEUS DESAFIOS

Como dito anteriormente, foi a busca/processamento das informações individuais permitiu, regulou e determinou a grande expansão da economia baseada em dados pessoais, pois diminuiu os gastos operacionais das empresas e melhorou seu desempenho.

A busca em massa por informações pessoais permite fabricar tecnologias preditivas, que trazem conforto e comodidade para o usuário, além de meios para que a empresa ofereça uma propaganda mais acertada. Mas isso depende do processamento e tratamento dos dados. Em meio essa busca que acontece de maneira desenfreada e a qualquer custo, ocorre um empenho ordenado dos indivíduos imperativa, com foco principal no consumidor, que permeia tanto a sua maneira de portar na rede como as suas atitudes mais habituais, chegando muito próximo até dos sentimentos, tornando o usuário quase, transparente.

Por isso, é preciso perceber que a mineração de dados afeta o cotidiano dos indivíduos, com ênfase no processo de submissão que esses usuários são submetidos, considerando as inúmeras atitudes automatizadas que esses têm que tomar e que definirão seus futuros.

Apesar da economia de dados pessoais ser atraente, ele pode nos propiciar promessas que possuem grandes ressalvas que a sociedade não considera tão graves, uma vez que são vistos como elementos longe de sua realidade. Neste capítulo, abordarei os resultados do total transparência das pessoas no mercado informacional, além dos desafios para atingir a efetiva autodeterminação.

2.1 Importância da proteção de dados

No smartfone, ao baixar um aplicativo, para que ele funcione da melhor maneira, é exigido o acesso aos contatos da agenda, ligações, arquivos do sistema, microfone, câmera e etc. Em busca da melhor experiencia com os serviços, abre-se mão da privacidade, tudo isso com a falsa sensação de ser gratuito, quando na verdade a pagamento é feito através troca implícita dos serviços pelos dados.

É nesse contexto que a sociedade informacional estabelece suas raízes. Segundo o Sergio Amadeu da Silveira (2017, p. 31):

> O processo de obtenção de dados dos cidadãos seja com relação ao consumo, seja com relação ao lazer e ao trabalho nos confunde e acelera a

> mercantilização da vida. Dessa forma, o capitalismo cognitivo é imaterial e cibernético, baseado nos fluxos de informação comunicados, capturados, processados e analisados.

Nesse sentido, não realizar a devida separação do espaço privado e espaço público retrataria o fim da privacidade em que os algoritmos começaram a ordenar a vida do indivíduo, decidindo sobre seu futuro. É nesse contexto que a autodeterminação informacional ganha destaque pois além de proteger os direitos individuais, também limita a atuação desenfreada das empresas na captação massiva dos dados pessoais e consequentemente restringe que o usuário sofra com diversas consequências, dentre as quais:

2.1.1 Consequências da não-proteção dos dados pessoais

2.1.1.1 Modulação

Com o crescente uso de notebooks e máquinas de processamento de dados, consequentemente levou ao aumento do uso de software baseado em algoritmos. Tais softwares estão sob controle de aviões em voo, nossas rotas no Waze, semáforos inteligentes, resultados de pesquisa do Google, postagens no Facebook. Ou seja, possuem poder de mudar as trajetórias do nosso dia a dia, delineia nossas ações e determina o que teremos acesso

A governança algorítmica surge nesse cenário. Isso porque, os algoritmos não são neutros e tomam decisões impostas por seus programadores. Portanto, eles devem ser abertos, o que significa que seus usuários devem ter acesso à cadeia de processos que compõem seu código. Caso contrário, eles se tornaram os verdadeiros legisladores em nossas vidas diárias.

A modulação é utilizada por empresas que possuem diversas tecnologias. Um deles é o que Eli Pariser (2012, p. 21) chama de filtro de bolhas, filtro de bolhas ou filtro invisível:

> Os algoritmos do mecanismo de pesquisa, plataforma ou site escolhem o que veremos ou a ordem em que veremos primeiro. Assim, os algoritmos filtram o que precisamos visualizar. Somos, portanto, modulados, colocados em uma bolha ou em um módulo. Talvez a metáfora mais adequada seja a gaiola digital, pois somos agrupados e distribuídos por algoritmos com pessoas com comportamentos, interesses e até ideologias semelhantes.

Segundo Sérgio Amadeu da Silveira, é possível considerar que os algoritmos do Facebook são formadores de guetos ideológicos. Dessa forma, ainda segundo o autor “como tal, eles não contribuem para a democracia, pois isolam posições, reduzem a diversidade e as

possibilidades de recombinação de opiniões. Ou seja, produz bolhas ou jaulas digitais porque segue a lógica do mercado de dados.” (2017, p.91).

A plataforma regista as atividades da pessoa, proporcionando uma representação visual dos elementos e prestações de serviço de sua rede publicitária. Se alguém quiser estourar uma bolha, terá que pagar financeiramente para que os amigos fora da bolha leiam suas postagens. Assim, as bolhas são perfis coletados e analisados de acordo com dados individuais do usuário.

A justificativa disso tudo é o rastreio pela “experiência aprimorada do usuário". De fato, a bolha eleva a ação publicitária. Os consumidores têm suas informações individuais compartilhadas para criar modelos "em tempo real" para comerciantes de anúncios na internet. Mas o prejuízo é ainda maior, pois os algoritmos limitam a liberdade e padronizam os conteúdos que você tem acesso. Nesse sentido, prejudicam a autonomia da informação e o desenvolvimento da personalidade, estragando a variedade cultural e nos coloca em condições de inferioridade em relação aos algoritmos.

2.1.1.2 Profiling

O profiling é a prática em que os elementos informativos de natureza pessoal de uma pessoa criam perfil sobre elas para tomar uma variedade de decisões baseadas em relação a esses padrões. Palavra da língua inglesa que significa um critério de decisão subjetivo, levando o indivíduo a decidir baseando-se não em uma racionalidade perfeita, mas em um impulso originado e decorrente de seus valores pessoais.

Tal prática pode prejudicar pessoas de certos grupos. Segundo relatório do Escritório do Alto Comissário das Nações Unidas para os Direitos Humanos (ACNUDH), (2021, p.22):

> O chamado “racial profiling”, ou “perfilamento racial” presente na abordagem das forças policiais que, de maneira seletiva, prendem, fazem buscas pessoais e operações de vigilância que geram taxas desproporcionais de aprisionamento da população de jovens negros. A abordagem viola seus direitos humanos, porque são baseados em generalizações e estereótipos e não em observações objetivas.

2.1.1.3 Incerteza do fluxo de dados

Um meio de instrumentos tradicionais o usuário substitui uma quantidade de pecúnia por uma ferramenta de consumo, exemplificando, vários itens de um carrinho tem um valor correto, tratando-se assim de um relacionamento entre duas partes e a transação é feita for meio

de dinheiro e bens.

Todavia, com o advento da economia digital os usuários não usam mais a moeda física para pagar produtos e serviço, mas sim permitem o uso de seus dados individuais, recebendo publicidade direcionada.

Assim, essa relação torna-se multilateral, pois acontece também entre os vendedores de publicidade que buscam, a fim de obter um retorno financeiro desse modelo econômico. Com essa sistemática, o usuário caba por se tornar também se torna um produto comercializável, pois seus dados individuais compõem a transação econômica supracitada.

Trata-se de um meio de negócios apoiado principalmente por publicidade comportamental. Primeiramente, o usuário é atraído para que possa usufruir de um serviço ou produto, em segundo lugar, recolhe as suas informações, em seguida, permite encaminhar mensagens publicitárias, que é a sua origem de lucros. Dessa forma os usuários não precisam pagar pecúnia por um produto ou serviço, o pagamento decorre do oferecimento de suas informações individuais.

Assim, o formato desse modelo econômico válida a atribuição de valores aos dos dados pessoais, tornando relevante a variação econômica da enorme variedade de produtos e serviços “gratuitos” disponíveis na Internet. Em vista disso, é na maioria das vezes aceito que o pagamento de muitos serviços e produtos seja feito usando as informações pessoais do usuário.

Em contrapartida, a pessoa envolvida realmente não tem ideia de qual será o valor real da transação. As diferentes formas de utilização de suas informações individuais são infinitas, principalmente na realidade de arrecadação massiva de dados. As possíveis perdas ou mesmo os lucros que tal atitude econômica pode gerar é desconhecida. Por meio da sistemática da economia da informação, é indefinido perceber como a disponibilidade de informação pessoal pode afetar seu proprietário e logo, o "preço" a ser pago pelo uso de um bem de consumo.

Dessa forma, o proprietário dos dados não tem certeza de como serão usados ou com quais outras informações serão incorporadas. Assim, qualquer inferência sobre o custo real da atividade econômica em questão não pode ser feita. Ademais, a junção de informações pessoais está em constante andamento, quando um produto ou serviço é usado, várias informações são inseridas e agrupadas, e o fluxo de informações que pode ser extraído delas é intangível.

2.1.1.4 Vigilância

Na sociedade informacional, a constante observação das atitudes das pessoas é o que o impulsiona a economia. Nesse sentido, os dados pessoas constituem a matéria-prima extraída

para a criação de riqueza, existe na verdade “varejo de dados pessoais”, segundo Sérgio Amadeu.

Para operar esse meio de negócio, existe uma completa rede de agentes que processam os dados pessoais dos consumidores, trabalhando de forma colaborativa para agregar cada vez mais dados com finalidade de tornar as mensagens publicitárias ainda mais eficazes. A ciência do marketing transforma esse escrutínio em conhecimento para aumentar a eficácia da publicidade veiculada em ambientes virtuais.

Assim, a onipresença da internet tornou possível a vigilância constante dos usuários, através dos recursos de câmeras, microfones e geolocalização, dos smartphones, notebooks e demais aparelhos eletrônicos.

Esse é um dos motivos pelo qual a aplicação Waze, que pega a geolocalização dos consumidores foi comprado pelo Google por um valor substancial de US $1,3 bilhão. Ou também, redes sociais como Facebook possuem a ferramenta de check-in para marcar lugares que frequenta.

Essas informações de geolocalização são extremamente valiosas. Pois ao mesmo tempo que podem dar margem para ter mais assertividade na publicidade baseada na localização do potencial consumidor, também pode despertar olhares de criminosos que utilizam dessa informação como meio para praticar os mais variados atos ilícitos que perpassam desde encontrar o melhor horário para furtar o domicílio do usuário, até um possível sequestro mediante extorsão.

2.1.1.5 Roubo de identidade

Existem vários graus de roubo de identidade que podem ocorrer. As instâncias comuns incluem o uso de suas informações para se inscrever em um cartão de crédito, fazer criar contas falsas, chantagear alguém que conhece ou aplicar o golpe de fishing. A ameaça de roubo de identidade é real a partir do momento que você tem contas em sites/aplicativos ou compartilha seus dados sem tomar os devidos cuidados na internet.

Segundo o site SailPoint, as estatísticas mostram que este tipo de crime cibernético está em ascensão. Uma pesquisa feita sobre cibersegurança feita com 262 executivos de TI, comprovaram que 32% desse total já teve incidentes de roubo de identidade, com quantidades que variam entre um milhão ou mais identidades digitais vazadas.

2.2 Desafios para atingir a autodeterminação informacional

Apesar dos dispositivos legais defenderem a anuência do usuário e colocá-lo como protagonista, existem barreiras cognitivas, estruturais e culturais que obstruem a possibilidade do usuário de autodeterminar seus dados pessoais. Dentre essas limitações temos que:

2.2.1 Decisão da utilidade subjetiva

As pessoas tendem a se concentrar em benefícios imediatos, que no entendimento e nos meios de negócios da economia da informação são representados pelo acesso a produtos ou serviços online. Por este motivo, qualquer dano à privacidade, não será levado em consideração temporariamente, desde que consiga acesso.

É inegável, o dano potencial associado à perda de fiscalização sobre dados individuais só pode ser sofrido no futuro. Por tal emento, os proprietários de dados pessoais buscam dar maior importância a esses benefícios imediatos, diminuindo os danos que podem resultar da perda do uso de suas próprias informações pessoais, ademais soma-se a isso que após escolher por essa opção, dificilmente o consumidor revogará o consentimento.

Segundo Ricardo Bioni (2021, p. 150):

> Nesse jogo de ganhos e perdas, as pessoas tendem a buscar uma "zona segura" da qual não se sintam culpadas pelos danos sofridos. Trata-se da chamada dissonância cognitiva, na qual o sujeito busca alívio para compensar simetricamente o desconforto. É nesse contexto que ocorre o chamado "paradoxo da privacidade". Em que pese as pessoas valorarem a proteção de seus dados pessoais, elas empreendem ações dissonantes a tal apreço. Há uma relação de inconsistência entre o que eles praticam e o que consideram idealmente.

Portanto, mesmo que as legislações coadunem para o fim de buscar a independência do consumidor, sobre a ideia de que ele inteiramente capaz de determinar o uso de deus dados pessoais é contraditória quando nos deparamos com a enorme complexidade que envolve o fluxo de dados pessoais, isso porque o usuário desconhece tais elementos o que aumenta sua vulnerabilidade.

Pelo exposto, cria-se uma situação visível de vulnerabilidade entre o usuário e as empresas publicitárias e navegadores de dados, demostradas por evidencias colacionadas ao longo desse trabalho.

2.2.2 Evidências empíricas

Nesse sentido, cria-se uma relação assimétrica de vulnerabilidade, havendo uma série de evidências empíricas a esse respeito, dentre elas temos quatro exemplos contidos na obra "Proteção de dados pessoais, a função e os limites do consentimento" de Ricardo Bioni:

2.2.2.1 Compreensão dos modelos de mentalidade

Nesse contexto, considerando o disposto até aqui é imprescindível discorrer acerca da compreensão dos modelos de mentalidades. De início com ênfase na mentalidade do proprietário de dados pessoais, o autor Ricardo Bioni traz em seu livro "Proteção de dados pessoais, a função e os limites do consentimento" uma pesquisa relevante na intenção de perceber qual é o meio de conhecimento dos proprietários de informações individuais relacionadas ao transporte de seus dados pessoais, desenvolvida pelas as pesquisadoras Lorrie Cranor e Aleecia McDonald das Universidades de Stanford e Carnegie Mellon.

As pesquisadoras que realizaram entrevistas a um grupo de indivíduos aleatório e constatando que somente 23% dos consumidores utilizam o meio de navegação privada (método simples parar bloquear a coleta dos dados pessoais), (BIONI, 2021, p.141).

Além disso, "somente 17% deletam cookies. Percebe-se, no plano da sua busca, a falta de conhecimento técnico dos usuários, mesmo em se tratando de métodos básico e principiais de segurabilidade dos dados", Ademais "70% das pessoas que foram ouvidas afirmaram que quando realizam compras online levam em conta se o site permitiria o compartilhamento de suas informações pessoais com outras empresas ligadas a publicidade" (BIONI, 2021, p.141).

Tal fator deixa visível que apesar dos consumidores não possuírem um conhecimento completo do fluxo de suas informações pessoais, se preocupam com o uso de suas informações. Assim, Bioni (2021. p. 142) ainda expõe por meio dessa pesquisa que:

> Essa preocupação com a proteção dos dados pessoais é coerente com o alto percentual de **64% dos entrevistados que consideraram ser invasiva a vigilância sobre as suas atividades on-line**. Fica evidenciado uma contradição, que ganha destaque quando os entrevistados são questionados, se pagariam o valor de U$ 1,00 (um dólar) para evitar que os provedores de Internet coletassem suas informações pessoais, ou, se aceitariam o desconto de U$ 1,00 (um dólar) em troca da permissão para que os provedores de Internet coletassem seus dados pessoais. Perceba que **apenas 11% afirmam estar dispostos a pagar o valor de U$ 1,00 (um dólar)**. Ao passo que, no

> segundo grupo, 69% concordariam com o desconto ofertado em troca de suas informações pessoais. Tais percentuais confirmam as limitações cognitivas expostas anteriormente.

Desta feita, é notório a ausência de entendimento referente ao funcionamento da sistemática de trafego de informações pessoais e da sua inclusão no ramo da publicidade comportamental. Nas palavras de Ricardo Bioni (2021, p.142): “tal estudo empírico sublinha a posição de vulnerabilidade dos cidadãos em exercer o controle de seus dados pessoais, o que perpassa desde uma assimetria informacional até a contradição de ideias”.

2.2.2.2 Constante inovação de tecnologias de rastreamento

Ademais, continuando a exposição de dados empíricos que contribuem para a elucidação do exposto nesse trabalho, Bioni traz em sua obra supracitada, um “segundo estudo empírico foi realizado pelos pesquisadores da Universidade de Berkeley da Califórnia. Realizou-se uma revisão da literatura dos trackers, testando-os em navegações simuladas nos 100 (cem) websites mais acessados nos Estados Unidos”. (2021, p.143).

Todavia, antes da exposição da pesquisa é imperioso definir o termo Tracker. Esse é um termo fornecido a uma categoria de softwares que armazenam os caminhos das atividades virtuais do proprietário de dados, e são mais difíceis de deletar ou bloquear que outras ferramentas. Conforme Ricardo, “A utilização de tais softwares, tornam a coleta de dados ubíqua, robusta e redundante. Isso porque, elas são mais difíceis de ser bloqueadas, pois são armazenadas de forma incomum em pastas locais do sistema computacional e por não ter uma expiração por padrão a cada término da sessão de navegação”. (Bioni, 2021, p.143).

Nesse contexto, a pesquisa supramencionada detectou que os trakers detinham a capacidade de reiniciar a atividades mesmo que sejam deletadas, executando novamente um programa que já foi desligado reativando-as automaticamente sem a necessidade de nenhuma de atividade por parte do usuário.

Desta feita, o resultado alcançado pelos pesquisadores e descrito por Bioni (2021, p.143) revela que:

> Dada essa metamorfose e sobreposição de rastreadores, eles continuam a perambular se não há o extermínio de todos eles pelo titular dos dados pessoais. Por exemplo, **se o usuário deleta cookies, ele ainda poderá ser rastreado por outros inúmeros trackers, flash, cookies, E-tags e assim por diante**. Essas novas tecnologias tornam, portanto, a vigilância mais opaca. Ela não só flui a cada passo e rastro da navegação do usuário, como, também,

> dribla as escolhas destes com relação à coleta de seus dados pessoais. Tais tecnologias empregam liquidez a um monitoramento contínuo e permanente dos usuários, acuando os em meio a uma corrida armamentista tecnológica que invalida as suas escolhas para que as suas informações pessoais não sejam coletadas. Esses dispositivos são as micro telas do século XXI que criam um estado de visibilidade constante do cidadão, colocando em xeque a sua capacidade de controlar seus dados pessoais.

Assim, com o mencionado estudo é indubitável que existe de fato a uma enorme vulnerabilidade do usuário frente as inúmeras tecnologias. Tal fato revela uma problemática que como relata Ricardo Bioni (2021, p.144):

> Mesmo que as normas legais elevem o consentimento como seu elemento normativo central e esteja em constante atualização legislativa, caso os consumidores não se capacitarem para o controle de seus dados pessoais, o próprio mercado acaba por criar novas tecnologias para esquivar da legislação e controlar os dados pessoais dos cidadãos.

Pelo exposto, é imprescindível que mesmo com o avanço das legislações, o usuário busque mais conhecimento para conseguir se esquivar dessas tecnologias maléficas.

2.2.2.3 Mercado da economia dos dados

Ademais, em referência ao mercado da economia dos dados, Ricardo Bioni trouxe ainda uma terceira pesquisa empírica realizada na Faculdade de Comunicação Annenberg da Universidade da Pensilvânia. Nela questiona-se se os consumidores estariam confortáveis e conscientes da troca de seus dados pessoais por serviços e produtos “gratuitos”, para tal fim:

> A pesquisa entrevistou 1.506 pessoas adultas de diferentes faixas etárias, classes socioeconômicas e etnias, a fim de ser a mais representativa possível da população americana. Na pesquisa foi constatado que 91% considerariam “injusta” a coleta de suas informações sem o seu respectivo conhecimento. Já no exemplo de um supermercado que proponha dar descontos em troca das informações pessoais que ele coleta a respeito de todas as suas compras, 43% concordariam com tal prática. O estudo associou essa reduzidíssima parcela da população, resistente em favor do câmbio-troca da economia dos dados pessoais, e chegou as seguintes conclusões: 84% gostaria de ter controle sobre o que é feito com os seus dados, e 65% reconhece que tem pouco controle sobre o que pode ser feito com as suas informações pessoais. (BIONI, p.144).

Diante disso, de início é possível perceber, nas palavras de Ricardo que os usuários desejam ter um maior controle sobre o uso de seus dados pessoais, reconhecendo, ao mesmo

tempo, que têm pouca gerência sobre tal situação.

Nesse sentido “O estudo coloca em xeque, a capacidade dos consumidores como sujeitos capazes de controlar as suas informações pessoais. No plano de fundo dessa constatação encontra-se o diagnóstico de que a prometida autodeterminação informacional é estrangulada em meio a uma relação assimétrica. (BIONI, 2021, p.145).

Dessa forma, como elucida Bioni (2021, p. 145):

> A programada autonomia dos consumidores para controlar seus dados pessoais é sufocada por todo um mercado sedento por tal ativo econômico. A lógica da economia dos dados pessoais prevalece e impõe as suas forças sobre a parte mais vulnerável dessa relação”. Então, os consumidores mostram-se impotentes para fazer valer o seu desejo de controlar seus dados pessoais, sendo tal assimetria de poder a mola propulsora de tal resignação.

Logo, está evidente a importância da identificação da parte vulnerável que como já discorremos ao longo desse trabalho é o usuário, que deve ser empoderado com o fim de reequilibrar essa relação cheia de desigualdades.

2.2.2.4 Transparência após regulamentação

Por fim mais não menos importantes o autor Ricardo Bioni trouxe ainda uma quarta pesquisa empírica acerca da transparência após a regulamentação que foi conduzida pela Universidade de Bochum (Alemanha), veja:

> Após notar um aumento exponencial dos avisos de cookies por parte de websites no cenário pós-GDPR, os pesquisadores analisaram se tais notificações promoviam, de fato, transparência acerca das práticas de tratamento de dados pessoais pelas plataformas e se, em última análise, auxiliariam na obtenção de um consentimento válido por parte dos usuários. O posicionamento do aviso em mais de 91,8% das vezes era alocado no topo ou ao final da plataforma, não sendo de fácil visualização. Na medida em que tais notificações não bloqueavam o conteúdo do site, consequentemente havia uma baixa da taxa de cliques. Ainda, uma boa parte era colorida de forma a prejudicar a sua visibilidade, como, por exemplo, tonalidades escuras. Os usuários entrevistados mostraram o quão desafiador é a construção de um vocabulário que seja de fácil compreensão, o próprio termo “cookies”, apesar de ser empregado em boa parte das notificações, é técnico e seu significado não é tão difundido. Outrossim, alguns dos entrevistados não compreendem as implicações das suas escolhas, como, por exemplo, acreditando que recusar um cookie os impediria de acessar o site ou significaria o aparecimento de menos anúncios. (BIONI, 2021, p. 146).

Assim, por todo exposto essa pesquisa deixa claro que é bastante eloquente e por isso perigoso o design de sites e redes a ponto e conduzir as atitudes tomadas pelos usuários, sendo necessário a criação de uma tecnologia com o fim de reduzir essas ferramentas em proteger o usuário.

2.2.3 Discursos Limitantes

Declarar que a intimidade é um direito que deve ser abdicado em favor das facilidades e comodidades que a tecnologia nos proporciona é importante para proporcionar um conformismo no usuário para que os agentes do mercado informacional possam coletar e manipular as informações pessoais sem deliberações.

Conforme afirmam, o fim da intimidade não é algo trágico, mas sim bem-vindo. Nessa visão, o fim da privacidade seja uma lavagem social de algo que não gera negócios lucrativos ou empreendimento como a capacidade de usar dados pessoais diariamente. Afinal, qual mal a economia de dados pode nos proporcionar?

Um exemplo claro de posicionamentos fim da proteção da privacidade é encontrado no artigo "A privacidade está morta e não é tão ruim quanto parece", escrito por André Santos, CEO da Predicta. Esse artigo indica que o mercado poderá oferecer melhores produtos e serviços se forem retiradas as barreiras e proibições da expansão do mercado. Quanto mais as empresas saberem sobre seus consumidores, mais seus produtos e serviços podem ser perfeitamente adaptados aos interesses individuais. Assim, o indivíduo abre mão de alguns direitos fundamentais advindos de sua condição de cidadão com o intuito de aperfeiçoar sua experiência como um ser comprador.

Nesse contexto citado, comprar é o que importa e a vida será reduzida à prática de consumir os produtos e serviços fornecidos pelas empresas. O que mais poderia valer a pena além da experiência do cliente?

Segundo Ricardo Bioni (2021, p. 145):

> A comercialização da vida pessoal, intimidade e afeto parece ser uma forte tendência na economia da informação baseada no mercado de dados. As corporações do capitalismo da informação disputam o mundo em que queremos viver. A guerra econômica é, portanto, também uma guerra estética. São tentativa de captura dos desejos que exigem antes a captura das informações dos seres desejantes. Para prever gostos, desejos, áreas de interesse, as empresas buscam as análises mais aprofundadas. Os dados pessoais são a matéria-prima deste processo.

Nesse contexto, é possível inferir que consideram a privacidade como algo relativo e antiquado que se deve conceder lugar para as novas e melhores experiencias. Ou seja, aparece como um direito ultrapassado.

Outrossim, ao olhar do ponto de vista da segurança e bem-estar, discursos como: "a privacidade é somente para pedófilos" reafirmam a ideia de que a restrição da privacidade é algo positivo, isso pois os criminosos terão mais dificuldade em esconder atividades ilícitas.

Essa linha de pensamento coaduno com declarações como: “Quem não deve não teme” ou “Não tenho nada a esconder de ninguém”. Infere-se que pessoas comuns não precisam se preocupar com sua privacidade, seus e-mails, seu histórico de navegação, suas ligações, porque só teria sentido caso tivessem algo a esconder.

Nesse contexto citado, a privacidade cria um grau desnecessário de insegurança social. Sua existência não apenas dificulta a coleta de dados pelo mercado, mas também facilita a atividade de criminosos que se escondem por trás das leis.

Portanto, o mercado informacional dissemina crenças limitantes que ressaltam a ideia de que a privacidade protege os criminosos e que com plena transparência dos dados pode haver menos corrupção, menos violência nas redes e mais razões para fazer o correto.

Em contrapartida, quando se trata dos segredos industriais, a segurança das decisões de negócios, a proteção da dinâmica algorítmica e o código fonte, ao contrário de exigir ou realizar o fim da privacidade, tem-se uma necessidade de mercado para a proteção de tais dados, isso pois alegam ser usados pelas empresas para manter o segredo dos planos de ações governamentais.

Isto é, as mesmas empresas e governos que exigem que os usuários sejam translúcidos com seus dados, também afirmam não pode ter seus códigos algorítmicos, negociais e industriais revelados para não se comprometer diante da concorrência de mercado.

Percebe-se uma evidente contradição de discursos que faz aflorar reflexões de como seria um mundo em que as verdadeiras intenções são sempre expostas, e que não haverá mais diferenciação entre o público e o privado.

Em suma, na sociedade informacional desenvolveu-se uma busca incessante por dados pessoais. Para que uma empresa tenha mais assertividade e poder no mercado, ela deve fazer a coleta massiva dos dados. Para facilitar essa coleta, lógica neoliberal cria discursos limitantes que buscam influenciar na tomada de decisão dos usuários.

Somado a isso, a deficiência cognitiva, estrutural ou técnica do indivíduo. Como se não bastasse, as empresas buscam cada vez mais desenvolver tecnologias com o intuito de enfraquecer ainda mais a parte o usuário em meio ao mercado da informacional.

Portanto, fica claro e evidente a hipossuficiência do proprietário dos dados pessoais. Nesse sentido é imperioso uma maior intervenção, seja dos atos normativos para que se empodere o sujeito vulnerável, seja na capacitação do titular dos dados para que tenha consciência e efetivo controle do seu consentimento. A ideia é elaborar estratégias que conscientize e instrua o sujeito, tido como vulnerável, para que saiba reconhecer situações de coleta massiva de dados, e possa alcançar sua efetiva autodeterminação informacional.

CAPÍTULO 3 – LGPD E SEGURANÇA DA INFORMAÇÃO COMO FERRAMENTA PRÁTICA DE PROTEÇÃO DOS DADOS PESSOAIS

Como foi demonstrado anteriormente, os dados possuem um alto valor ativo. Diante disso, as empresas partem para uma busca desenfreada dessas informações. Em meio a isso tudo, está o titular dos dados, que vive uma relação assimétrica de vulnerabilidade. Por isso, é necessário, maior comprometimento com a autodeterminação informacional para que não haja lesão ao direito à privacidade, como também, para que ele não sofra com as consequências da automação, que pode influenciar diretamente em seu futuro.

O ideal é uma integração entre as áreas técnica (segurança da informação) e jurídica (LGPD), pois a proteção de dados só é verdadeiramente efetiva quando vem acompanhada de segurança da informação. Dispositivos legais como a LGPD normatizam no sentido da autonomia e da política do consentimento do usuário. O Art. 7º da LGPD diz que: O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; [...].

Segundo Jimene (2020), a segurança da informação já existia anteriormente à necessidade de proteção de dados pessoais. Porém, era focada na proteção de informações sigilosas e estratégicas relevantes para os negócios. É válido dizer então aquela máxima: “Nem todo incidente de segurança da informação é uma violação de dados pessoais. Mas toda violação de dados pessoais é um incidente de segurança”.

No contexto dos dados pessoais, a segurança da informação tem como responsabilidade proteger o negócio contra riscos e incidentes como vazamento de dados, ataques cibernéticos e indisponibilidade. Para isso, trata da análise de vulnerabilidades, adequação e automatização de processos, prevenção à fraude etc. Ou seja, trabalha para que os dados não tomem finalidade diversa das que foram recolhidos.

De acordo com Jimene (2020), devem ser utilizadas medidas técnicas e administrativas que possibilitem a proteção de dados pessoais de acessos não autorizados e de circunstâncias acidentais ou ilícitas de destruição, perda, alteração, compartilhamento ou divulgação.

Vê-se então, que a adequação à LGPD passa obrigatoriamente por procedimentos relacionados à tecnologia da informação, tendo em vista o alto volume de dados armazenados em sistemas informatizados, que devem ser tratados com medidas e técnicas de segurança.

Mais do que estratégica, a segurança da informação é essencial para a proteção do conjunto de dados da corporação, pois, seus métodos objetivam viabilizar e assegurar a

disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. É vital para qualquer empresa conhecer os seus dados e restringir o acesso, além de saber onde estão sendo transmitidos, armazenados, compartilhados.

A utilização de recursos tecnológicos que possibilitem a segurança da informação no ambiente digital é necessária para que sejam cumpridas as obrigações legais de tratamento de dados pessoais e seja garantida a privacidade dos titulares. São alguns exemplos de mecanismos tecnológicos que contribuem para a segurança da informação e, consequentemente, para a proteção de dados: ferramentas de autenticação de acesso, recursos de criptografia, assinatura digital e certificação digital (JIMENE, 2020).

Portanto, é importante ter consciência do cenário em que estamos inseridos, de supervalorização dos dados pessoais e hiper conectividade dos usuários, para que se construa uma cultura de gestão de segurança da informação no Brasil. Só assim, será possível efetivo respeito aos direitos fundamentais e redução nos riscos de ataques e mau uso dos dados pessoais.

3.1 Formas de obtenção dos dados dos usuários

Bruce Schneier (2018, p. 33), pesquisador em segurança da informação, define seis tipos de dados pessoais baseados em plataformas de redes sociais online:

> dados de serviços, fornecidos para abrir uma conta; dados divulgados, inseridos voluntariamente pelo usuário; e dados confiáveis, como comentários de usuários, dados incidentais, que contêm informação sobre as ações que os utilizadores realizam durante a utilização de um website e são utilizados por publicidade direcionada; e dados inferidos, que são as informações trazidas de atividades, perfis e dados.

Para capitar tais dados, as plataformas utilizam de vários métodos, dentre eles incluem indisponibilizar os recursos de um sistema (DoS), enganar o usuário (phising), o monitoramento desautorizado da máquina (spywares), sequestro de dados (ransomware) e etc.

3.1.1 Cookies

De início, a fim de elucidar cabe definir o que são cookies. Trata-se de minúsculos pacotes de dados mandando de um site para o navegador do usuário. Assim, A cada retorno a um site, o navegador manda o cookie novamente ao servidor, que guarda o histórico de

navegação daquele indivíduo específico.

Nesse contexto, as empresas de tracking realizam acordos com os sites para anexarem seus cookies. Dessa forma, elas rastreiam a navegação dos usuários o que permite saber quando um indivíduo está buscando certo site.

Pelo exposto, cookie pode ser definido, segundo Jule Hintzbergen (2017, p. 74), como:

> Um identificador de ações feitas na web. Alguns cookies instalados em dispositivos podem durar cerca de dois anos. Desse modo, são usados por uma empresa que quer oferecer um produto ou serviço para um certo perfil de consumidor. Por isso, a visualização do produto surge em banners em todos os sites que esse tipo de consumidor navega.

3.1.2 Clickstream

Ademais, é necessário para uma elucidação mais completa definir o termo clickstream, também chamada de sequência de cliques. Refere-se a um método de registro do caminho que o indivíduo percorre ao acessar em uma página da internet ou aplicativo do celular.

De outro modo, diferentemente os cookies são empregados para guardar os dados do indivíduo e grava-los em um servidor da web. Assim analisando os dois conceitos, clickstream se revela importante porque classifica as atividades das pessoas na web, tornando viável inclusive, testar a produtividade dos empregados de uma empresa.

3.1.3 Deep Packet Inspection

Deep Packet Inspection é mais uma forma de obtenção de comportamento de navegação do usuário, mais abrangente, entretanto que as demais. Como suas características, a inspeção profunda de pacotes ou deep packet inspection. Isso ocorre quando um provedor de serviço de internet inspeciona o conteúdo dos pacotes de dados que entram e saem dos endereços IP que distribui para seus usuários navegarem na internet.

Vale ressaltar que esse dispositivo, foi usada por Phorm, uma agência de publicidade no Reino Unido, em parceria com provedores de internet, para segmentar anúncios. Entretanto, um dos problemas mais recorrentes desse elemento é que toda a ação realizada pelo usuário na rede é captada. Um clique em um link, uma senha, absolutamente tudo que se faz na rede é armazenado pelo deep packet inspection. Essa e outras ferramentas anteriormente citadas nos permite inferir que, o mercado articula técnicas invisíveis aos indivíduos para obter seus dados e vendê-los para as empresas.

3.1.4 Geolocalização

Outrossim, cabe ainda falar do fenômeno da Geolocalização no contexto abordado nesse Trabalho de Conclusão de Curso. Isso porque, a captura de dados e de imagens que revelam os ambientes externos e internos realizada por milhões pessoas nos mais variados aplicativos é mais uma forma de captação de dados dos usuários que como já foi demonstrado tem um elevadíssimo valor.

Nesse contexto podemos citar o fenômeno do Pokémon Go que se revela um de como as artes digitais foram e estão sendo colocadas a serviço da coleta de informações pessoais e da ampliação da microeconomia da interceptação de dados.

Tal elemento demonstrou que um número elevado das plataformas de entretenimento está incluindo um modelo de negócios baseado na gratuidade dos serviços em troca da venda de suas preferências e possibilidades de captura de dados dos usuários. Permitindo assim a captura do padrão de comportamento, perfil de consumo, e lugares requentados pelos usuários nas cidades.

3.2 Métodos para proteção dos dados através da LGPD

Para atingir o consentimento válido e eficaz a LGPD estabelece princípios a ser observados, impõe limites para a coleta de dados e cria obrigações para que a empresa esteja sempre atuando com o consentimento do usuário.

Caso não cumprir com seus comandos, haverá a responsabilização do órgão. Dentre elas estão:

> **Advertência, multa ou até mesmo a proibição total, ou parcial de atividades relacionadas ao tratamento de dados**. As multas podem variar de 2% do faturamento do ano anterior até a R$ 50 milhões, passando por penalidades diárias. A Lei também prever a obrigação de divulgação de incidentes, a eliminação de dados pessoais e a inversão de ônus da prova a favor do titular do dado. (SÁ, 2019, p. 18).

Também estabelece direitos aos titulares de dados, segundo a LGPD, em seu artigo 9º e 18º:

> 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...
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: **II - acesso aos dados; II - correção de dados incompletos, inexatos ou desatualizados; IX - revogação do consentimento**, nos termos do § 5º do art. 8º desta Lei.

Cria a Autoridade Nacional de Proteção de Dados (ANPD), que tem como suas atribuições:

> O estabelecimento de padrões técnicos, a avaliação de cláusulas e jurisdições estrangeiras no que tange a proteção de dados, a determinação para a elaboração de Relatórios de Impacto, a fiscalização e aplicação de sanções, atividades de difusão e educação sobre a lei, bem como demais atribuições que visam a correta aplicação da lei e os princípios da proteção de dados pessoais. (Lei nº13.709/2018, Art. 55).

Com os mandamentos citados acima, as empresas que realizam qualquer tipo de processamento de dados pessoais do usuário deverão se adequar as exigências da LGPD. Nesse contexto, necessitarão que destinar tempo e dinheiro em sistemas de *cibersegurança* e *compliance*.

Entretanto, como dito anteriormente a decisão legislativa de colocar sobre o indivíduo a grande responsabilidade de oferecer seu consentimento não é a melhor estratégia. É nesse cenário que a segurança da informação ganha destaque, pois, com seus fundamentos, irá capacitar o usuário para proteger seus dados de maneira eficaz.

3.3 Métodos para proteção dos dados através da segurança da informação

Atualmente, considerando o maior número de informações acessíveis nas redes, a atitude de indivíduos com intenções ruins pode ser imensamente mais fácil, apesar da existência de várias tecnologias, como por exemplo a criptografia, que busca preservar a privacidade dos usuários. Por isso, além dessas tecnologias é imprescindível também uma ação por parte do usuário com o fim de fortalecer a proteção de seus dados, enumeraremos aqui algumas delas.

3.3.1 Crie senhas fortes

Para usar a internet com mais segurança e tranquilidade, buscando diminuir os riscos de

invasão, um dos passos iniciais é desenvolver uma senha forte, independente da atividade, seja nas redes sociais, cadastros de empresas ou e-mail, pois assim é evitável o furto de dados dos usuários e acesso de pessoas indevidas a informações de natureza pessoal.

Segundo a especialista Vanessa Fetter (2020, p. 102): “O termo senhas ‘fortes’ inclui a inserção de símbolos; Alternância de letras maiúsculas e minúsculas. Combinações com mais de 7 caracteres; Uso de números diversos, além de não usar número de telefone, nome de usuário e data de nascimento”.

Assim, com ações de pequenas demandas como essa, criando uma senha mais difícil e robusta o usuário protege seus dados e dificulta o acesso a suas informações.

3.3.2 Desconfie de sites que pedem dados pessoais

O termo Phishing, refere-se à ação de pescar dados. Nesse contexto, a ferramenta é usada para alcançar o usuário através de uma mensagem de uma mensagem de texto, e-mail ou página web que busca o indivíduo, organizações e bancos de dados. É na verdade uma infração tecnológica utilizada para furtar informações intimas, como senhas de cartões de crédito. números do CPF, RG e outros.

Conforme estabelece Haans Baars, “para não cair nessa prática e manter a proteção dos dados pessoais é preciso sempre desconfiar de mensagens de e-mails, sites e mensagem que solicitam o preenchimento de informações pessoais” (2017, p.44).

Nesse contexto, é bastante recorrente que os indivíduos acreditem no phishing, graças ao maior poder de convencimento das mensagens, que carregam um aspecto de confiabilidade. Ainda conforme o Hanns supracitado, “os usuários recebem uma mensagem com oferta especial ou até premiações oportunas, em troca de fornecimento de suas informações pessoais em formulários” (2017, p.45).

Todavia, a prática supracitada vai para além do furto de informações privadas, soma-se a isso o intuito de atingir bancos de dados de Estados e empresas, ação conhecida como spear phishing, essa ação em 2015 foi responsabilizada por 38% dos ataques corporativos, ocasionado o rombo de mais de $1,8 milhões, segundo o site The Economist.

3.3.3 Antivírus

Outrossim, Jule e Kees (2017, p. 30) alertam em sua obra “fundamentos de segurança da informação” sobre os vírus, que de acordo com eles:

> Os vírus podem ser captados de variadas formas. A título de exemplo podemos citar um simples cupom de desconto de uma loja, nele é possível constatar a presença de códigos que interferem no funcionamento dos computadores. Assim, o antivírus é capaz de identificar a entrada do vírus, realizando procedimentos de quarentena e remoção do código, automaticamente. Atualmente, há programas que alertam os usuários, requisitando o escaneamento da máquina. **Dessa forma, antivírus é um software que detecta e impede a atuação de programas maliciosos, que podem corromper o sistema de máquinas, além de roubar dados de usuários.** Ou seja, é uma tecnologia que foca em prevenção e segurança.

Nesse contexto, é relevante que o consumidor realize a busca de período em período do seu computador, e atualize o antivírus, buscando se resguardas as ameaças da internet.

3.3.4 Redes Sociais

O grande alcance das redes sociais proporcionar com que homens e mulheres começassem a usar essas redes para dividir suas informações privadas. Nesse sentido cresceu muito a exposição exagerada das pessoas e suas vidas pessoais o que gera fatores negativos, com a exposição desnecessária de dados pessoais. A título de exemplo podemos citar os comentários negativos em fotos e vídeos que causam problemas psicológicos, como baixa autoestima, aumento da ansiedade e depressão. Nesse sentido o especialista Hans Baars (2017, p.125) afirma que:

> Por isso, para dificultar a prática criminosa online e offline, além de usufruir de uma boa saúde mental, a dica é incluir apenas o essencial nas redes. Há também algumas opções de privacidade que as plataformas oferecem, como a restrição de compartilhamento, divisão por grupos e alertas de segurança.

Pelo exposto, é viável ao dividir dados nas redes sociais os usuários restrinjam a amplitude da publicação usando elementos das próprias redes para buscar mais privacidade e controle sobre o alcance das suas informações pessoais.

3.3.5 Backup periódico

Backup é cópia segura de seus arquivos. Com esta ação, você pode evitar a perda de seus dados pelo resto de sua vida devido a ataques de vírus, hackers e cibercriminosos em seu computador.

Atualmente, há plataformas que permitem aos usuários fazer backup de seus dados diretamente na nuvem, dando-lhes ainda mais segurança. Além da possibilidade de acessar os arquivos de qualquer local com acesso à internet, não há risco de deterioração do HD, falha de leitura e etc.

3.3.6 Webcam e o Microfone

Por fim, mais não menos importante temos que citar o cuidado necessário com a Webcam e Microfone, isso porque hackers invadem maquinas o tempo todo para terem acessibilidade aos mais variados elementos e informações do usuário. Nesse sentido caso consiga acessar a câmera ou microfone do aparelho os invasores podem ouvir e ver toda a atividade interna do consumidor, ensejando posteriormente em contundas mais graves. Dessa forma o cuidado com tais dispositivos é fundamental, o uso de adesivo já é uma boa opção para barra o uso da câmera pelos criminosos.

CONCLUSÃO

Assim, diante de todo o exposto é possível concluir que em um intervalo muito curto de tempo os elementos tecnológicos transformaram a vida em sociedade nos mais variados aspectos e elementos. A criação da internet e a inserção de novas tecnologias, como câmeras fotográficas portáteis e smartfones, por exemplo, colocou fim nas barreiras físicas de comunicação.

Nesse sentido, em uma sociedade informacional, tudo está conectado e gera dados. Por isso, é possível afirmar que os dados se tornaram o grande tesouro da atualidade e aqueles que têm acesso aos bancos de dados podem ser considerados detentores de um sistema de poder. Exemplo disso é o que foi evidenciado no caso Snowden, em que a NASA realizava vigilância em massa no mundo inteiro, sob a justificativa da segurança nacional e do combate ao terrorismo.

Assim, diante da abrangência e do domínio sobre os dados das pessoas, nasce uma preocupação acerca de como esses dados serão usados. Surge então, a necessidade de regulamentação. Perpassam três gerações de leis, que vão desde a concentração do poder totalmente na mão do Estado, até o estágio atual que se concentra todo em torno do consentimento do titular dos dados.

A LGPD defende o tratamento de dados pessoais na internet de forma democrática, segura e transparente. Todavia, mesmo diante de tais disposições da LGPD, todos podem estar sujeitos a ação de hackers e pessoas mal intencionadas, que podem infringir a segurança e roubar os dados pessoais.

Além disso, é preciso perceber que mesmo que o consentimento seja o núcleo das relações de coleta e tratamento dos dados pessoais, ainda assim, o usuário vive uma relação de vulnerabilidade devido suas limitações cognitivas, estruturais e culturais. Assim como também, o mercado está em constante evolução para criar meios de conseguir coletar os dados a qualquer custo.

Tal fato foi evidenciado no documentário “O Dilema das Redes” (2020), dirigido por Jeff Orlowski, que promoveu reflexões alarmantes sobre o uso das redes sociais e as ações estratégicas agressivas das empresas que dominam a área. Nesse contexto, os usuários são as vítimas potenciais dessa estrutura na qual os dados atropelam as pessoas em carne e osso.

Soma-se a isso as crenças limitantes criadas pelo mercado informacional visando manipular o indivíduo e coletar seus dados. Tais teorias, defendem a transparência total dos dados dos usuários para aperfeiçoar sua experiencia online, pois dessa maneira as empresas

conseguem mais assertividade em oferecer seus produtos e serviços. Todavia, a vida não pode ser reduzida à prática de consumir, e como foi citado anteriormente a completa transparência no compartilhamento dos dados pessoais pode trazer sérias consequências.

Percebe-se então, o tamanho da assimetria informacional que deve ser superada para que haja uma efetiva autodeterminação informacional. Os atos normativos que visam a proteção de dados pessoais, como a LGPD, se demonstram pouco eficaz na prática. Isso pois, mesmo que tais dispositivos normativos busquem a autonomia e o consentimento, eles partem da ideia de que o indivíduo detentor dos dados é, via de regra, um sujeito racional, livre e capaz de entender o mercado informacional. Fato esse que não coaduna com a realidade devido as limitações do indivíduo e formas de opressão do mercado, citadas anteriormente.

Dessa maneira, o tiro saiu pela culatra, o que inicialmente nasce com o fundamente de ser forma eficaz de garantir a proteção dos dados pessoais, se tornou uma forma de legitimar a captação de dados na economia digital. Nesse sentido, na prática, o consentimento considera-se uma verdadeira ficção jurídica, na medida em que não se enquadra no contexto social em que vivemos.

Mais do que garantir artificialmente diferentes padrões de consentimento, acima de tudo, devem ser buscadas outras ferramentas regulatórias para equilibrar as assimetrias referenciadas dos mercados de informação. Este é o maior desafio: dar aos cidadãos mais controle sobre seus dados, uma autonomia real.

Nesse sentido, os atos normativos necessitam ser modificados visando o empoderamento dos usuários ao em vez do consentimento em sua formula mais pura. É preciso repensar as disposições normativas para que interfiram no próprio fluxo informacional, não deixando, apenas, sobre os ombros dos titulares dos dados pessoais, o fardo normativo da proteção de dados pessoais.

Deve-se então, buscar limitar o poder de negociabilidade dos direitos da personalidade, para impedir que o próprio titular dos dados se torne um produto e acabe “coisificado”. A autonomia da vontade deve ser, portanto, limitada, assegurando-se que o fluxo informacional seja apropriado para o livre desenvolvimento da personalidade. (Bioni, 2021, p.140).

Vale ressaltar que a arquitetura da rede, muita das vezes é projetada para limitar a autonomia da vontade. Técnicas são utilizadas pelas empresas para solicitar o consentimento do usuário de forma disfarçada, confusa, redundante. Assim sendo, é preciso impor novas formas para operacionalizar a solicitação do consentimento, levando-se em conta todas as vulnerabilidades citadas neste trabalho, de forma que fique mais claro e objetivo.

Outrossim, o empoderamento deve ser feito principalmente para além dos termos legais,

tendo em vista que o meio informacional está sempre em constante modificação, dessa forma, fica inviável manter as legislações sempre atualizadas para abarcar todos os métodos de captação de dados. Por isso, é mais eficaz capacitar o usuário para reconhecer e estar preparado para os diversos tipos de ataques que possa sofrer, seja com uma atitude positiva (fazer) ou negativa (não-fazer).

É nesse contexto que a segurança da informação ganha destaque, pois não se trata de uma estratégia regulatória puramente liberal para que o sujeito consiga sair da zona de vulnerabilidade. Ela oferece ferramentas práticas para o indivíduo se proteger, que vão desde métodos mais simples como excluir os cookies ou usar navegador com aba anônima até as mais complexas como analisar se o site que você está acessando é falso.

Por fim, é importante que a sociedade se desprenda das crenças limitantes e se torne um usuário ativo e crítico, para que não se despersonalize e torne uma massa de manobra para mercado informacional. Nesse contexto, a tecnologia pode ser incorporada a vida das pessoas para facilitar e trazer mais conforto, todavia, esses benefícios não devem ser sobrepostos em detrimento do direito à privacidade. Atitudes como: de restringir o alcance das publicações, recusar que o aplicativo acesse sua geolocalização, rejeitar os cookies quando necessário expressam esse senso crítico.

Com isso, o indivíduo estará preparado para reconhecer os riscos e, caso queira, dar (ou não) seu consentimento de maneira válida. Só assim, será possível reduzir essa assimetria que o mercado informacional criou e racionalizar um processo de tomada de decisão genuíno.

REFERÊNCIAS

ABREU, Karen Cristina Kraemer. **Tulipas vermelhas:** uma (re)leitura das relações na (e da) Internet (p. 38 – 47). IN: Synthesis – Revista de Produção Científica da FACVEST: os vários olhares da produção científica. Lages/SC: Papervest Editora, n. 5, jan/jun. 2004.

ARAÚJO, J. C. (Org.). **Internet & Ensino:** novos gêneros, outros desafios. Rio de Janeiro: Lucerna, 2017.

BIONI, Bruno Ricardo. **Proteção de dados Pessoais – A Função e os Limites do Consentimento**. Rio de janeiro: Ed. Forense, 2021.

BRASIL. **CONSTITUIÇÃO FEDERAL DE 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 21 out. 2020.

BRASIL. **Lei de Acesso à Informação**. Disponível em: https://www.google.com/search?q=lei+de+acesso+%C3%A0+informaLei+de+Acesso+Infoma.0.0l6. Acesso em: 24 nov 2020.

BRASIL. **Lei Geral de Proteção de Dados.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em 14 dez. 2020.

BRASIL. Lei n. 12.737/12. **Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Extraído de: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 03 de nov. 2020.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 de nov. 2020.

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais: lei n. 13.709/2018. 2019**. 50 f. TCC (Graduação) - Curso de Direito, Centro Universitário de Brasília - Uniceub, Brasília, 2019.

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

FORTINET – Fortinet Threat Intelligence Insider Latin America. **Incidentes de segurança cibernética: soluções de segurança.** Califórnia-EUA, 2020. Disponível em: https://www.fortinetthreatinsiderlat.com/pt/Q4-2019/BR/html/trends#trends_position. Acessado em: 02 de jan. de 2021.

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

GARCIA, Bruna Pinotti. **Ética na internet: um estudo da autodisciplina moral no ciberespaço e seus reflexos jurídicos.** Dissertação (Mestrado em Direito) – Programa de Mestrado em Direito, Fundação de Ensino "Eurípedes Soares da Rocha". Centro Universitário Eurípedes de Marília – UNIVEM, Marília, 2013.

HOUAISS, A.; VILLAR, M. de S.; FRANCO, F. M. de M. **Dicionário Houaiss da língua portuguesa.** Rio de Janeiro: Objetiva, 2009. 1986 p. Contém CD-ROM completo (armazenado na seção de multimeios).

JIMENE, Camilla do Vale. **Da importância da segurança da informação para adequação à LGPD.** In: BLUM, Renato Opice (Org.). Proteção de dados: desafios e soluções na adequação à lei.Rio de Janeiro: Forense, 2020.

LIMA, Caio César Carvalho em ***LGPD: Lei Geral de Proteção de Dados Comentada***. Coordenadores: Viviane Nóbrega Maldonado e Renato Opice Blum.2ª Edição. TR Revista dos Tribunais. São Paulo. 2020. pg. 181

MENEZES, Elias Jacob de Neto, DE MORAIS, Jose Luis Bolzan. **Análises computacionais preditivas como um novo biopoder:** modificações do tempo na sociedade dos sensores. Rio Grande do Norte: Novos Estudo Jurídicos, 2018.

MENDONÇA, Renata**. Como os testes de Facebook usam seus dados pessoais - e como empresas ganham dinheiro com isso.** 2018. Disponível em: <http://www.bbc.com/portuguese/salasocial-43106323>. Acesso em: 25 dez. 2020.

PARISER, Eli. **The Filter Bubble: What the Internet is Hiding from You**. Londres: Penguin UK, 2011.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: Comentários à lei 13709/2018 (LGPD)** – São Paulo; Ed. Saraiva Educação, 2019.

SÁ, Marcelo Dias de. **Análise do impacto da nova lei de proteção de dados pessoais nas aplicações de internet das coisas**. Brasília, 2019.

SAWAYA, S. M. **A leitura e a escrita como práticas culturais e o fracasso escolar de crianças de classes populares:** uma contribuição crítica. 1999. Tese (Doutorado em Psicologia) – Instituto de Psicologia, Universidade de São Paulo, São Paulo, 1999.

SILVEIRA, Sergio Amadeu. "**Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais**". Liinc em Revista, São Paulo: Edições Sesc São Paulo, 2017.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados).** Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/ PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 26/12/2020.