

**CENTRO UNIVERSITÁRIO  
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE**

**FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE**

**A TUTELA DOS DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO À LUZ  
DA LEI Nº 13.709/2018**

Letícia Sayuri Uemura Sukino

Presidente Prudente/SP  
2019

**CENTRO UNIVERSITÁRIO  
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE**

**FACULDADE DE DIREITO DE PRESIDENTE PRUDENTE**

**A TUTELA DOS DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO À LUZ  
DA LEI Nº 13.709/2018**

Letícia Sayuri Uemura Sukino

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação do Prof. Wilton Boigues Corbalan Tebar.

Presidente Prudente/SP  
2019

**A TUTELA DOS DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO À LUZ  
DA LEI Nº 13.709/2018**

Monografia aprovada como requisito  
parcial para obtenção do Grau de  
Bacharel em Direito.

**Banca Examinadora**

---

**Wilton Boigues Corbalan Tebar**  
**Orientador**

---

**Ana Laura Teixeira Martelli Theodoro**  
**Examinadora**

---

**João Victor Mendes de Oliveira**  
**Examinador**

Presidente Prudente/SP, 06 de novembro de 2019.

## **AGRADECIMENTOS**

Primeiramente, agradeço aos meus pais, Iraci Harumi Uemura Sukino e Mario Mitsuaki Sukino, por nunca deixarem me faltar nada, por terem me oportunizado o acesso à graduação no curso de minha escolha, que sempre mostraram que a educação é o caminho certo a ser trilhado, sempre presentes e dispostos a auxiliar no que fosse possível, independente do que for. Este trabalho certamente não existiria sem o apoio deles.

Ao meu professor e orientador Wilton Boigues Corbalan Tebar, por ter aceitado me orientar durante esta trajetória, por todo o conhecimento transmitido ao longo deste ano. Agradeço pela paciência, pela compreensão e por ter se disposto a ajudar sempre que precisei.

Agradeço aos examinadores, por terem aceitado a compor a banca e a estarem presentes, obrigada por terem se disponibilizado a fazer parte desta etapa da minha graduação, que está prestes a ser concluída.

Por fim, agradeço à todos que me acompanharam durante esta trajetória, me motivando e incentivando para que tudo isto pudesse ocorrer da melhor forma possível.

## RESUMO

O presente trabalho busca, através de análises à sociedade da informação, de acordo com sua estrutura e funcionamento, como as novas tecnologias da informação são capazes de violar de forma silenciosa, direitos fundamentais da pessoa humana. O objetivo desta pesquisa é destacar a importância da proteção de dados pessoais, salientando sua natureza de direito da personalidade, de forma a compreender o porquê de sua valorização dentro da economia digital, destacando ao titular de dados pessoais, o porquê deve preocupar-se com este bem jurídico que lhe pertence. O conflito de interesses entre controladores de bancos de dados e os interesses individuais de cada usuário se mostram em desequilíbrio, uma vez que este é hipossuficiente nesta relação jurídica. A economia digital cresce constantemente, e a ciência jurídica deve tomar medidas legais para evitar violações a direitos da pessoa humana. O trabalho utiliza o método dedutivo para o enfrentamento de tais premissas.

**Palavras-chave:** Sociedade da informação. Direito à privacidade. Proteção de dados pessoais. Consumidor de vidro. Lei Geral de Proteção de Dados Pessoais.

## **ABSTRACT**

The present monographic work sought, through analysis over the information society, according through your structure and operation system, how the new information technologies are able to violate, in a silent way, fundamental rights of the human person. The objective of this search was to highlight the importance of the personal data protection, pointing out your nature as personality rights as a way of comprehending the reasons that lead to your valorization inside the digital economy, specially about the holder of the personal data, making him worry about the legal good he owns. The conflict of interest between database controllers and individual interests of each user, shows that is an uneven relation, and the user itself, is in a weaker position. The digital economy is growing constantly, and the legal science has to take legal measures to prevent violations of human person's rights.

**Key-words:** Information Society. Right to privacy. Personal data protection. Glass consumer. General law of personal data protection.

## SUMÁRIO

<b>1 INTRODUÇÃO</b> .....	<b>7</b>
<b>2. SOCIEDADE DA INFORMAÇÃO</b> .....	<b>11</b>
2.1 A Economia da Informação .....	13
2.2. Do Crescimento do Alcance da Tecnologia aos Diversos Públicos .....	17
2.3. O Consumidor Online .....	18
<b>3 A INTERNET E SEUS IMPACTOS JURÍDICOS</b> .....	<b>22</b>
3.1. O Histórico da Internet.....	22
3.2 Relações da Internet com o Direito .....	24
3.3 A Internet e sua Regulamentação .....	28
3.3.1 Legislação pertinente .....	29
<b>4 INTERESSES DIFUSOS</b> .....	<b>35</b>
4.1. Direito à Privacidade .....	35
4.1.1 Interpretações acerca do direito à privacidade.....	38
4.2 Direito à Informação .....	40
4.3 Direito à Proteção de Dados Pessoais .....	41
<b>5 A RELEVÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS E SUA APLICAÇÃO PRÁTICA</b> .....	<b>45</b>
5.1. No que Consistem os Dados Pessoais .....	49
5.2 A Estratégia Mercadológica dos Negócios Online: o Modelo Freemium .....	50
5.2.1 A monetização dos serviços e produtos online .....	52
5.3. A Publicidade Direcionada Online .....	55
<b>6. O CONSUMIDOR DE VIDRO</b> .....	<b>59</b>
6.1 O Controle do Consumidor por Meio de Seus Dados Pessoais .....	60
6.2 O Caso Target.....	62
6.3 O Caso 23andme .....	63
6.4 O Caso Cambridge Analytica .....	65
6.5 O Caso FaceApp.....	69
6.7 A Problemática dos Dados Pessoais e sua Extensa Gama de Alcance .....	71
<b>7. OS MEIOS DE TUTELA DOS DADOS PESSOAIS</b> .....	<b>75</b>
7.1 Tecnologias de Controle de Privacidade.....	77
7.2 A Autoridade Nacional de Proteção de Dados Pessoais (ANPD) .....	82
7.3 O Regulamento Geral Europeu de Proteção de Dados (GDPR).....	86
7.4 Agência de Acesso à Informação Pública da Argentina .....	87
7.5 Os Desafios da Aplicação Eficaz da LGPD no Brasil .....	89
<b>8 CONCLUSÃO</b> .....	<b>91</b>
<b>REFERÊNCIAS</b> .....	<b>96</b>

## 1 INTRODUÇÃO

As relações sociais passaram por grandes transformações nas últimas décadas, especialmente no que diz respeito aos meios utilizados para que elas venham a se efetuar.

Houve a gradual substituição de meios físicos, como o papel, com as cartas, para possibilidade de comunicação em tempo real, como o telefone, evoluindo para e-mails, mensagens de texto, vídeo chamadas, e tantos outros mecanismos que foram surgindo ao longo do tempo.

Neste sentido, foi desenvolvida uma das mais utilizadas tecnologias de transmissão de dados em todo o mundo, a internet. Todavia, ela não foi apenas uma novidade que se tornou conhecida, muito além disso, revolucionou o modo como a sociedade se organiza, seja como uma forma de comunicação mais eficiente, como também, de extrema importância no aspecto econômico, diante de inúmeras startups de tecnologia que puderam crescer e criar um mercado jamais visto, desde a ideia de vendas inteiramente online, assim como tomadas de decisões do processo de produção baseadas em análise de dados.

Em análise aos processos elencados exemplificativamente acima, verifica-se o grande potencial de alcance das tecnologias da informação, que trouxeram o surgimento de novas relações sociais e jurídicas, capazes de causar grandes impactos na vida das pessoas, seja em âmbito individual, seja em âmbito empresarial.

A ideia deste trabalho foi, através de pesquisas exploratórias acerca destas novas relações jurídicas, demonstrar que a ciência jurídica deve maior atenção ao tema devido à sua constante presença na vida da sociedade atual, a qual difere-se de todas as outras que existiram até então, pois baseia-se em um intenso fluxo de informações, que são transmitidas de maneira rápida e eficiente.

Neste sentido, houve relutância acerca de parte dos estudiosos, que visualizavam as lides oriundas da internet como algo passageiro, ao qual poderia ser aplicada a lei geral. Todavia, a doutrina que se especializou nesta temática passou a compreender a complexidade do tema, pois não se tratava de algo passageiro.

Com a análise das relações provenientes da aldeia digital acompanhada de todos os seus frutos, verifica-se a sociedade da informação. A



partir dela nasce a economia da informação, que passa a ser uma espécie de commodity, de valor tão elevado, capaz de definir o poder que um Estado possui perante a economia mundial, baseado na quantidade de qualidade de informações que ele detém.

Desde a década de 1990, quando teve início a popularização das redes, sua evolução ocorreu de forma constante, sendo cada vez mais acessível a todos os públicos. A World Wide Web está cada vez mais presente em todas as relações sociais da atualidade, e diante de sua infinita gama de aplicações, uma versatilidade jamais vista antes, e a ciência jurídica deve atentar-se a ela.

Entre os principais direitos cuja natureza é diretamente afetada pelas relações digitais, encontram-se o direito à privacidade, de informação e de proteção de dados pessoais.

As principais discussões versam a respeito do direito à privacidade. Isto porque trata-se de uma garantia fundamental que acompanhou a evolução da sociedade com os séculos, com enfoque em sua aplicação na autodeterminação informacional.

Todavia, embora seja uma garantia consolidada e reconhecida por maioria consolidada dos Estados, não vem se mostrando como a tutela adequada do cidadão pela ótica do direito digital. Isto posto, seria hipótese de tutela por meio do direito à proteção de dados pessoais.

O direito à proteção de dados pessoais abarca a dinamicidade da sociedade da informação, onde cada informação do sujeito irá compor sua projeção dentro do mundo virtual, independente de lugar, tempo e causa. Além disso, conforme a arquitetura em que as redes foram projetadas, os usuários não possuem controle sobre o trajeto de seus dados, muito menos sobre suas aplicações e fins que podem ser utilizados.

Isto posto, é realizada uma análise de acontecimentos da sociedade da informação que demonstram a importância do dado nas vertentes atuais. A versatilidade do uso de dados mostra que ele tem infinitas aplicações, desde uma análise de consumidor de uma marca a influências políticas por direcionamento de informações. O poder encontra-se nas mãos daquele que melhor aplicação de dados fizer diante de seus interesses.

Por conseguinte, o valor da informação ainda é objeto de inúmeras controvérsias, isto porque sua monetização foge do padrão convencional de

negócios, uma estrutura que fornece serviços em formato que não exige pagamento em espécie para ser utilizado, mas isso não significa que existe a gratuidade dos serviços.

A partir deste novo formato que aparenta não exigir contraprestação, o presente trabalho se propõe a explorar o funcionamento dessa estratégia mercadológica, de forma a explicar as razões que proporcionaram o crescimento exponencial dos serviços e produtos oferecidos de forma online, que está intimamente ligado à proteção de dados pessoais.

O titular dos dados pessoais, por sua vez, pode ser considerado um consumidor de vidro, devido à transparência dos seus dados pessoais e a falta de controle que possui sobre a trajetória dos mesmos. O papel passivo do usuário o torna volúvel a qualquer uso que seus dados tenham, cuja as consequências podem se manifestar direta e indiretamente.

Considerando a visão pluralista de aplicabilidade dos usos possíveis dos dados pessoais, o presente trabalho se propôs a apresentar acontecimentos atuais que envolvem a ideia do uso controlado dos dados e como eles são capazes de influenciar um sujeito ou até toda uma nação.

Neste contexto, a visão atual acerca de dados informacionais não é capaz de salientar sua importância para a sociedade atual, fincada na velocidade e acesso a tudo, apesar de suas benesses, o descontrole acerca de informações pessoais pode implicar em danos irreversíveis em um cenário de caos.

Em virtude do que foi mencionado, buscou-se ainda, apresentar os diferentes meios de proteção que possuem o poder de serem efetivos, ainda que a passos lentos, em prol da constante evolução da sociedade da informação.

A metodologia aplicada neste estudo foi a dedutiva, analisando a essência dos dados pessoais, partindo de constatações particulares e caminhando em direção a vertentes mais abrangentes. Além disso, o método histórico foi utilizado, de modo a compreender a evolução da sociedade, seus novos institutos e mercados, para melhor elencar a forma da vida social atual, em busca de proporcionar o melhor entendimento acerca de seus efeitos em face a novos bens jurídicos a serem tutelados.

O trabalho teve como base a pesquisa doutrinária, legislação nacional e estrangeira, artigos científicos a respeito, reportagens jornalísticas e sites de

pesquisa, focados em transmitir diferentes ideias e pontos de vista acerca do direito digital.

## 2 SOCIEDADE DA INFORMAÇÃO

Com o advento de tecnologias que proporcionam a propagação rápida e instantânea de informações, teve início o que hoje se denomina a sociedade da informação. De forma rápida e direta, pode ser descrita como fruto da infraestrutura da informação.

A evolução tecnológica dos meios de comunicação sempre objetivou uma Aldeia Global, onde pessoas de qualquer lugar do mundo pudessem ter acesso simultâneo à notícia, ao fato divulgado.

Adiante, foram somados outros fatores, como a necessidade de corte de gastos, onde grandes empresas buscavam conectar suas atividades, e para isto, investindo em comunicação interna. Diante disso, os executivos foram capazes de poupar tempo, papel, viagens e especialmente, dinheiro.

Todavia, os investimentos em comunicação não se restringiram a uma mera economia, pois além disso, abriam um novo mercado, permitindo logísticas diferenciadas, o comércio online, possibilitando vendas personalizadas, e instituindo o princípio do estoque zero.

Um dos pioneiros neste mercado foram os chamados “home brokers”, o universo financeiro necessitava de mecanismos os quais fossem capazes de dinamizar operações e facilitar a evolução do mercado de ações de forma segura, já que envolve movimentações significativas e com a necessidade da segurança para seus usuários, com a segurança de dados que será analisada adiante.

Todavia, a aldeia digital, ambiente no qual, pela primeira vez, inúmeros indivíduos foram capazes de agir no mesmo período de tempo, também proporcionou grandes consequências decorrentes do comportamento irracional do mercado.<sup>1</sup>

A partir daí, foi gerada a necessidade de levar este benefício aos lares, quando teve início a instalação do computador em casa, para trazer o consumidor ávido para este novo universo que logo então estaria recheado de informações, produtos e serviços.

---

<sup>1</sup> Neste sentido: “Se, por um lado, é muito bom estar conectado, por outro o comportamento irracional de mercado afeta a todos, onde quer que estejam, de maneira nunca antes experimentada”. In: PINHEIRO, Patricia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2015, p. 68. *E-book*.

Realizando uma análise do ponto de vista histórico, Renato Martini<sup>2</sup> utiliza da ideia dos *enclosures acts*<sup>3</sup> que ocorreram no século XVIII na Inglaterra. Os cercamentos foram evento de grande impacto social e econômico, pois transformou terras que antes possuíam uso comum para realizar pastagens de ovelhas. Os camponeses expulsos, migraram para cidades, e os *gentrys*,<sup>4</sup> enriqueceram com a lã das ovelhas, que por fim, somada a migração com matéria prima, teve como resultado a Primeira Revolução Industrial.

Com esta análise, Renato Martini enxerga da mesma forma, com a intensidade do movimento, as incertezas, consequências, impactos dentro da sociedade, sejam na forma de laborar, da sociedade se organizar, da forma como a riqueza passa a ser vista, dizendo que:

A sociedade da informação e do conhecimento é sem dúvida um capítulo a mais no processo de industrialização que começa na Europa ocidental e se planetariza ao longo do século 20. As transformações geradas pela indústria e a técnica já apontavam decisivamente para ruptura da vida tradicional<sup>5</sup>

As mudanças cujo advento das tecnologias da informação trouxeram à sociedade, estão ocorrendo constantemente, e de acordo com o tempo em que estão sendo desenvolvidas, afinal, a evolução é inevitável, sendo apenas limitadas pelas técnicas de sua época para que estas possam evoluir mais rapidamente em menor período. A sociedade, ao sentir-se à vontade com as técnicas que possui, busca cada vez mais meios de aplicação delas em busca de inovação, pois é inerente do ser humano, em relação a novas ideias e perspectivas, fugir da inércia em busca de algo novo.

A sociedade da informação ostenta como ideia base a capacidade de transmissão de dados, que muitas vezes se traduzem em informações, com um tempo e quantidade nunca vistos, onde o fluxo informacional não encontra mais barreiras geográficas, onde um simples toque aos aparelhos celulares, na tecla do computador, torna possível o acesso a um endereço digital de qualquer lugar do mundo.

---

<sup>2</sup> MARTINI, Renato. **Sociedade da Informação**: para onde vamos. 1ª Ed. São Paulo: Trevisan, 2017. *E-book*.

<sup>3</sup> Lei dos Cercamentos de Terras (tradução livre)

<sup>4</sup> Nobreza que por seu poder, entendeu que cabia a eles realizar os cercamentos.

<sup>5</sup> MARTINI, op. cit.

Apesar dessa premissa, é preciso analisar que se trata de inovação que possui um pouco mais de três décadas, período no qual houve grande mudança, partindo do ambiente científico, onde a tecnologia era utilizada apenas por órgãos de alta patente, para o ambiente comum, altamente difundido e tornando-se um direito da população.

Embora seja um mecanismo de união, difusão de obstáculos, a sociedade da informação acaba por segregar aqueles que não se encontram inseridos e preparados para este universo, tal como expõe Patricia Peck:

O fenômeno de marginalização social se dá pela incapacidade dos indivíduos de conhecer e dominar as novas tecnologias — não basta saber escrever, é preciso saber enviar um e-mail. Ao mesmo tempo que a Era Digital abre maiores possibilidades de inclusão, a exclusão torna-se mais cruel. Aqueles que não tiverem existência virtual dificilmente sobreviverão também no mundo real, e esse talvez seja um dos aspectos mais aterradores dos novos tempos <sup>6</sup>

Logo, a principal ideia a ser auferida deste novo conceito é a mudança de ideias e perspectivas que o homem possuía diante do mundo: a velocidade, a quebra da barreira espaço-tempo e a mudança nas interações sociais ao redor do globo.

## 2.1 A Economia da Informação

Dentro da sociedade atual, a informação tornou-se um produto tão importante economicamente como commodities, tais quais minérios, grãos, petróleo. Mas diferente destes produtos, a informação, que pode ser traduzida por conhecimento, é considerada um bem público, mas não pertencente a um único estado soberano, e sim ao globo como um todo.

A principal característica de um bem público, certamente é que estes não são passíveis de apropriação, ou se possível, existe grande dificuldade para que isto ocorra. <sup>7</sup>

Conforme o entendimento de Bruno Ricardo Bioni, a informação é o (novo) elemento estruturante de (re)organização da sociedade, tal como fizeram a

---

<sup>6</sup> PINHEIRO, Patricia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2015, e-book.

<sup>7</sup> Stiglitz, Joseph E. **The revolution of information economics: the past and the future**. Disponível em: <https://www.nber.org/papers/w23780.pdf>. p. 4. Acesso em: 26 fev. 2019.

terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial.<sup>8</sup>

O entendimento de Renato Martini segue esta linha de pensamento:

A informação é um fenômeno de proporções muito sugestivas para a vida social, uma vez que se articula com a presença da tecnologia e avança decisivamente em infraestrutura com as redes. Tornou-se comum dizer que a informação é algo que, ao se dividir, seu conteúdo não se diminui em absoluto, como é no mundo dos átomos, ao inverso: expande-se e cresce, multiplica-se<sup>9</sup>

Existe então, uma nova forma de manipulação dos dados necessários, onde deixou-se de lado a ideia manual e o armazenamento e acúmulo de informações mudaram de forma, saindo principalmente do papel, no formato de átomos, ocupando espaço físico e utilizando do método da escrita, era feita a condensação de conhecimento e dados necessários. E este foi o recurso mais utilizado para tal fim, até a chegada dos bits, que podem ser definidos como:

A bit (short for "binary digit") is the smallest unit of measurement used to quantify computer data. It contains a single binary value of 0 or 1.

While a single bit can define a boolean value of True (1) or False (0), an individual bit has little other use. Therefore, in computer storage, bits are often grouped together in 8-bit clusters called bytes. Since a byte contains eight bits that each have two possible values, a single byte may have 28 or 256 different values<sup>10</sup>

A partir de então, seu uso passou a ser altamente difundido, tendo sido o início ao uso dos computadores de maneira geral, e foram sendo inclusas funções que aprimoram sua utilização como fonte de armazenamento e busca, tal qual a pesquisa por palavras-chaves.

---

<sup>8</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2018, p. 5.

<sup>9</sup> MARTINI, Renato. **Sociedade da Informação**: para onde vamos. 1 ed. São Paulo: Trevisan, 2017. E-book.

<sup>10</sup> Bit Definition. **Site Tech Terms**. Disponível em: <https://techterms.com/definition/bit>. Acesso em 28 fev. 2019

Um bit (abreviação de dígito binário) é a menor unidade de medida utilizada para quantificar dados de computador. Ele contém o valor binário de 0 ou 1.

Quando um único bit consegue definir o valor booleano de Verdadeiro (1) ou Falso (0), o bit individual tem outros usos. Assim sendo, no armazenamento de computador, bits geralmente são agrupados em conjuntos de 8-bit aglomerados, denominados bytes. Como um byte contém oito bits que, individualmente possuem dois valores possíveis, um único byte pode ter 28 ou 256 valores diferentes. (tradução livre)

Assim, houve mudança exponencial no modo como se visualizava a informação, tal como Bruno Bioni expõe:

Dessa forma, os bits desmaterializaram a informação, permitindo a sua introdução em computadores. E, com o passar do tempo, todo tipo de informação passou a ser digitalizado, tal como o áudio e vídeo.

Isso implicou em virada exponencial na quantidade de informações processadas. Com a linguagem binária, permitiu-se um acúmulo de informações inimaginável e em novas plataformas – *e.g.*, *compact disk (CD)*, *pen drive*, computadores pessoais, etc. – em comparação ao suporte primitivo dos átomos (papel) <sup>11</sup>

A utilização de novos meios para realizar o armazenamento de informações, o qual, mesmo antes do advento da internet, a ideia da concentração de dados como forma de potencializar o crescimento econômico se mostrou latente e cada vez mais necessário.

O taylorismo, por exemplo, teve como objeto, o processo de produção em si, investindo em treinamento para seus operários em busca de aumento de produtividade. Deste modo, reconhece-se a importância da informação como fator decisivo na produção de riquezas desde a Revolução Industrial.

Este sistema organizacional de produção, foge à ideia de uma empresa somente, realizar todo o processo para manufaturar o bem de consumo, e parte para estruturação em conjunto de empresas que atuam colaborativamente, com funções pré-estipuladas, de forma que a atividade empresarial seja descentralizada e horizontal.

Um exemplo a se citar é a multinacional do ramo do vestuário: a Zara. Neste sentido, tem-se o seguinte:

[...] fortes investimentos são realizados em TI, eliminando as distâncias em que se encontram clientes e fornecedores e colaboradores. A empresa funciona em tempo real com um excelente gerenciamento de TI, utiliza-se o código de barras que permite o monitoramento do produto ao longo das diversas etapas do processo de produção, distribuição e entrega às lojas, onde começa o ciclo de comunicação. O sistema de TI permite a troca constante de informações pela cadeia de suprimento, entre consumidores e gerentes de loja, entre gerentes de loja, especialistas de mercado e 11 estilistas, entre estilistas e equipe de produção, entre compradores e terceirizadas, entre gerentes de depósito e distribuidores, oferecendo um

---

<sup>11</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2018, p. 7.



excelente sistema facilitador para coordenar e exercer a governança por parte da empresa.<sup>12</sup>

Os lojistas da Zara registram suas vendas e compartilham dados com o centro de criação da marca em La Coruña. E através de análise de mercado, conforme os produtos mais aprovados pelos consumidores, após esta retroalimentação terá início uma nova leva de produção de itens para abastecerem as lojas considerando os dados de consumo de seus clientes.<sup>13</sup>

Bioni conclui que a informação em si não é o que alavanca eficiência na atividade empresarial, mas o seu processamento-organização a ser transformado em conhecimento aplicado.<sup>14</sup>

No âmbito empresarial, a utilização dos hábitos de consumo dos clientes, além dos dados pessoais, possibilita formas mais eficientes de empreender, pois permite, junto ao seu público, analisar quais medidas tiveram maior sucesso, sejam em concepção de produto, forma de apresentação da publicidade para promover o item no mercado.

Neste sentido, Marcel Leonardi diz que o avanço da tecnologia, aliado ao aumento da velocidade das redes e à melhoria dos mecanismos de busca, gera mais atividade econômica baseada na economia da informação.<sup>15</sup>

A informação, portanto, é instrumento a ser examinado utilizando dos mecanismos certos para que possa ser transformado em estratégia. É fonte a ser lapidada de forma inteligente e utilizando dos parâmetros mais adequados a cada finalidade desejada, onde os dados pessoais de clientes, usuários da rede são convertidos em mecanismo de produção de riquezas, sendo a matéria prima da atualidade.

---

<sup>12</sup> GOMES, Silvia Maria; RODRIGUEZ, Carlos Manuel Taboada. **Configuração de cadeia de suprimentos**: estudos de casos em ambiente dinâmico de competição. Disponível em: [https://www.aedb.br/seget/arquivos/artigos08/164\\_164\\_seget.pdf](https://www.aedb.br/seget/arquivos/artigos08/164_164_seget.pdf). Acesso em: 28 fev. 2019.

<sup>13</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro, 1. ed: Forense, 2018, p. 10.

<sup>14</sup> BIONI, op. cit., p. 11.

<sup>15</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1. ed. São Paulo: Saraiva, 2012, p. 68.

## 2.2 Do Crescimento do Alcance da Tecnologia aos Diversos Públicos

Diversos fatores influenciaram a grande difusão da internet na sociedade uma vez reconhecida a grande capacidade de revolucionar o modo como as relações sociais se dão.

Os procedimentos que a internet utiliza beneficiam outras mídias, tais como televisão, rádio e imprensa, as quais viram neste mecanismo, uma nova janela para divulgar aquilo que já tinham consolidado em suas plataformas tradicionais.

Primeiramente, os primeiros passos foram o crescimento da infraestrutura no que diz respeito às telecomunicações ao redor do globo. As empresas do ramo instalaram rádios, satélites, cabos, chegando à mais recente fibra-ótica. Acompanhando a constante ampliação da estrutura, o barateamento de equipamentos tais como computadores e notebooks, inclusive a expansão de crédito auxiliara neste aspecto.

Seguidamente, houve propagação de tecnologias móveis, popularizados através de smartphones e tablets, com grande variedade de modelos, tamanhos, custos, reduzindo de dimensões e deixando de lado a exclusividade do acesso utilizando apenas computadores e laptops, e passando a ser portátil a todo tempo. Atualmente, em muitos países o acesso à internet utilizando de aparelho móvel ultrapassa a navegação feita utilizando computador.

Por fim, atualmente existe a chamada “internet das coisas”, no que se refere a dispositivos, especialmente eletroeletrônicos, tais como televisores, caixas de som, consoles, os quais também tem acesso à rede por si só, criando a possibilidade de uma casa completamente conectada e automatizada, mercado que vem conquistando cada vez mais público.

Os aspectos citados acima foram de suma contribuição para a universalização da internet nas últimas décadas, todavia, eles sozinhos não são os responsáveis por conquistar o público on-line.

O que de fato foi capaz de atrair a atenção das pessoas para utilizar este meio, pode ser dado mérito às startups, que são empresas novas, que apresentam projetos inovadores, ligados à pesquisa, criação e desenvolvimento de novas ideias, e neste caso, são especialmente aquelas que trazem seus produtos e serviços ao público online.

Diante das startups é possível citar o Dropbox, uma gigante que começou como uma pequena empresa, e trouxe a ideia do armazenamento em nuvem, apresentando novo modo de utilização da web, fornecendo um serviço que utiliza da lógica do “freemium”, que será tratado posteriormente.

As redes sociais ganharam grande poder de influência, como extensão que possibilita estabelecer novos relacionamentos, tais como Facebook e WhatsApp, além de expandir a ideia da comunicação via internet utilizando das tecnologias atuais, tais como chamadas de áudio, vídeo e mensagens de texto. Mídias sociais como Instagram e Youtube, trazem novas maneiras de consumir, criar e tomar conhecimento daquilo que está “em alta”.

O Netflix trouxe proposta inovadora, com o streaming de seriados, animações infantis e filmes, e posteriormente incluiu material de produção própria, fortalecendo-se no mercado, fazendo parcerias com fabricantes de eletrônicos para que seu conteúdo pudesse ser reproduzido em novas plataformas.

Uma das maiores revoluções, sem dúvidas foram as ferramentas de busca, onde a Google ganhou grande relevância. O mecanismo revolucionado pela Google, trouxe uma nova visão e perspectiva para o que a internet iria a se tornar a partir dela, onde estar conectado não se limitou a ser mero entretenimento e ganhasse espaço de ferramenta necessária para o dia a dia, seja para fins pessoais ou profissionais.

Através desta análise, é possível concluir que houve uma gradual evolução no que diz respeito ao acesso à internet e os serviços que esta passou a fornecer, fazendo com que o público consumidor se torne cada vez maior e relevante.

### **2.3 O Consumidor Online**

O usuário das redes, ao entrar em contato com os serviços que as mídias digitais lhe fornecem, torna-se um consumidor, o consumidor online. Estas pessoas, quando presentes nas redes, podem utilizá-la da forma mais democrática de acesso à informação já existente, isto porque os dados disponíveis na rede ao público em geral, incluem qualquer classe socioeconômica, idade e gênero, basta que tenha os meios que gerem o acesso.

É um público extremamente variado, e em especial nas redes sociais, a condição de equidade se mostra mais evidente. Existem todos os tipos de pessoas buscando entretenimento, utilizando ferramentas de busca, consumindo textos, fotos e vídeos de mídias sociais, sejam estas produzidas profissionalmente ou por amadores, amigos, entre os quais a mídia é compartilhada e ganha um maior alcance.

Todavia, o perfil comum dos usuários varia conforme o país em questão, especialmente analisando fatores como o nível de desenvolvimento econômico, que comumente acompanha um maior uso da internet, incluindo o fator geracional, uma vez que as novas gerações, também chamada de geração dos *millennials*<sup>16</sup> ou geração Y, já estão crescendo dentro de uma sociedade mergulhada no ambiente digital.

Dentro das redes, existe uma infinita gama de opções disponíveis ao usuário, partindo da busca por informação. Ele tem consciência de que a internet é fonte de (conteúdo útil), sendo as ferramentas de busca, o instrumento necessário para encontrar o que deseja.

Através da ferramenta, o usuário insere o conjunto de palavras chave que irão direcioná-lo aos resultados disponíveis e compatíveis com a instrução desejada. É um modo facilitador muito difundido na sociedade, uma vez que é um recurso muito utilizado no cotidiano das pessoas, sejam para buscas rápidas ou complexas.

Um exemplo disso é quando se trata de dúvidas a respeito de um estabelecimento, tal como um restaurante, ao procurar informações sobre ele na ferramenta de busca, é possível encontrar sua localização, avaliações de outros clientes, visualizar fotos do local, preços, entre outros fatores. Uma notícia vista rapidamente no telejornal, desejando informações mais específicas, o indivíduo recorre à ferramenta de busca, podendo encontrar matérias em informativos online a respeito, e até vídeos no Youtube, que retratem o dado procurado.

As pessoas buscam constantemente as informações mais variadas, tornando as ferramentas de busca, mecanismo indispensável. Mas este processo não envolve somente este tipo de serviço, uma vez que outras espécies, as quais se consolidaram no tipo de informação que são capazes de fornecer, tais como o

---

<sup>16</sup> Pessoa que nasceu entre 1980 a 1990.

YouTube para mídias de vídeo e áudio, o LinkedIn, consolidado como uma espécie de rede social para relações profissionais.

Com a utilização constante dessas plataformas, ocorre que o usuário passa a se fidelizar a determinado serviço quando necessita suprir interesse específico. Desta forma, conforme os acessos e utilização do consumidor, a plataforma é capaz de gerar um banco de dados a respeito de cada usuário.

Neste sentido, Claudio Torres expõe o seguinte:

A internet criou um ciclo virtuoso, a grande oferta de conteúdo atrai os consumidores, que suprem suas necessidades de informação, atraindo mais produtores de conteúdos, que atentem a outros nichos, atraindo ainda mais o consumidor <sup>17</sup>

Mas a internet não se restringe a uma mera fonte de informações. O usuário também busca entretenimento, seja esse por meio de vídeos, jogos, serviços de streaming.

A evolução dos dispositivos de captura e programas de edição de mídia e áudio, juntamente com o aumento de velocidade de acesso, permitiram que a produção deste tipo de mídia fosse amplamente difundida. As mídias digitais se mostram um ambiente democrático onde o produtor de conteúdo pode ser desde o amador a aquele que possui um estúdio com estes fins. Foi retirada a exclusividade das grandes mídias, tais como emissoras de televisão, dando visibilidade a pequenos produtores e amadores para produção de conteúdo online.

Além disso, estas mídias realizam grande trabalho em gerar praticidade para seu consumidor. O smartphone, que vem superando os acessos até mesmo por meio de computadores, vem sendo foco dos serviços de streaming, por exemplo.

O Spotify, substituindo os antigos arquivos em MP3, compra de CDs e downloads, é uma plataforma online que permite ouvir incontáveis músicas gratuitamente, mas com interrupções de publicidade, ou por um valor fixo, além de permitir o usuário realizar o download das músicas que desejar na plataforma, para poder acessá-las inclusive quando estiver offline.

O Netflix, também apresentou o *streaming* voltado para documentários, séries e filmes, que podem ser acessados a qualquer momento, em qualquer dispositivo de mídia que possua o acesso. E devido ao seu crescente número de

---

<sup>17</sup> TORRES, Claudio. **A Bíblia do Marketing Digital**. 2. ed. São Paulo: Novatec, 2018. e-book.

usuários, e vem sendo apontada como uma das grandes causas da perda de consumidores dos pacotes de televisão por assinatura.

Por fim, a internet também trouxe a possibilidade de o usuário estabelecer relacionamentos. A comunicação instantânea instalou na sociedade o crescente processo do relacionamento online.

No Brasil, uma das ferramentas marcantes na comunicação online foi o “MSN”, fornecido pela Microsoft, utilizado nos computadores em geral. Com a evolução dos smartphones, o WhatsApp ganhou campo, e junto ao Messenger, o envio de mensagens de texto online ganhou campo, trazendo cada vez mais funções, como mensagens de voz, mensagens de vídeo, chamadas de áudio e vídeo, sendo estrutura completa e substituiu o uso das chamadas de telefone, um dos meios de comunicação instantânea mais utilizados até então.

As redes sociais integram comunidades, aproximando pessoas que estão distantes geograficamente, e permitindo a comunicação 24 horas por dia. Neste caso, o consumidor muitas vezes foi compelido a utilizar a plataforma porque seu grupo de amigos está fazendo uso dela, criando um grupo para troca de informações, de forma que ele utiliza a rede para estar conectado com a comunidade.

Diante deste posicionamento, Carlos Torres expõe que ao suprir a necessidade de relacionamento do consumidor, a internet criou espécie de cola, que cria a necessidade de o consumidor estar sempre conectado e atualizado.<sup>18</sup>

Após esta análise, é possível verificar a presença onisciente da internet através das redes sociais no cotidiano das pessoas na sociedade atual, tornou-se ferramenta indispensável. A partir disso, serão analisados os efeitos jurídicos que este uso é capaz de gerar.

---

<sup>18</sup> TORRES, Claudio. **A Bíblia do Marketing Digital**. 2. ed. São Paulo: Novatec, 2018. *e-book*.

### 3 A INTERNET E SEUS IMPACTOS JURÍDICOS

A internet mostra-se na sociedade atual, como instrumento indispensável para as relações sociais que sustenta, além de possuir uma grande estrutura que se baseia nela para produzir efeitos. Neste capítulo, será abordada a história deste mecanismo, de modo a entender o seu funcionamento, os impactos jurídicos que ela apresenta, demonstrando as razões para que o universo jurídico verifique sua relevância e o modo que se encontram as previsões legislativas que versem acerca do tema.

#### 3.1. O Histórico da Internet

A internet surgiu no final dos anos cinquenta e começo dos anos sessenta como um projeto de pesquisa militar americano, o chamado ARPA: *Advanced Research Projects Agency*<sup>19</sup>, durante o período da guerra fria.

O projeto foi criado com a intenção de ser uma resposta à Ex- União Soviética pelo lançamento do Sputnik, tendo como ideia principal, conectar o Pentágono com os mais importantes centros universitários de pesquisa americanos com a finalidade de troca de informações rápidas e sob proteção, além de também proporcionar ao país uma tecnologia que conseguiria manter canais de comunicação mesmo com uma eventual guerra nuclear para que a rede de comando americana não fosse interrompida. Por trás deste grande projeto, existem grandes nomes que impulsionaram o projeto ARPA, trazidos por António Machuco Rosa:

Apresentamos aqui evidência histórica sobre o papel inspirador que membros fundadores do movimento cibernético, como Norbert Wiener e Warren McCulloch, tiveram em pioneiros da Internet como Joseph Licklider e Paul Baran. Licklider foi talvez o principal impulsionador do projecto ARPANET, que levaria à implementação da primeira rede física de computadores ligados entre si, precisamente a rede ARPANET, que foi a primeira rede da rede de redes que viria a ser a Internet (sob a evolução da Internet, cf. Hafner e Lyon, 1996, Abbate, 1999). Contribuindo para o nascimento das ideias guias do projecto existiram as relações pessoais documentadas entre Wiener e Licklider.<sup>20</sup>

<sup>19</sup> Agência de Pesquisa de Projetos Avançados (tradução livre)

<sup>20</sup> ROSA, António Machuco. **As origens históricas da Internet**: uma comparação com a origem dos meios clássicos de comunicação ponto a ponto. Disponível em: <http://www.ec.ubi.pt/ec/11/pdf/EC11-2012Mai-05.pdf>. P 103. Acesso em: 28 mar. 2019

Certamente, eles não podiam imaginar o engrandecimento que este projeto teria até chegarmos aos dias atuais.

Posteriormente, o projeto Arpanet da agência de projetos avançados (Arpa) do Departamento de Defesa norte-americano confiou, em 1969, à *Rand Corporation* a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a corrente de comando dos Estados Unidos.

A ideia utilizada foi a criação de pequenas redes locais (LAN), estrategicamente posicionadas em locais espalhados pelo país, as quais eram coligadas por meio de redes de comunicações utilizando a tecnologia WAN (*Wide Area Networks*<sup>21</sup>). Diante de um ataque nuclear, utilizando das redes conexas, que formavam a Internet, isto é, Inter Networking, literalmente, coligação entre redes locais distantes garantiria a comunicação entre as remanescentes cidades coligadas, conforme Liliane Minardi Paesani expõe:

No entanto, a decolagem da Internet ocorreu no ano de 1973, quando Vinton Cerf, do Departamento de Pesquisa avançada da Universidade da Califórnia e responsável pelo projeto, registrou o (protocolo TCP/IP) Protocolo de Controle da Transmissão/Protocolo Internet; trata-se de um código que consente aos diversos networks incompatíveis por programas e sistemas comunicarem-se entre si <sup>22</sup>

Ainda durante a década de 70, houve o desenvolvimento da ferramenta e-mail (*eletronic mail*<sup>23</sup>), que proporcionou o primeiro passo dos pesquisadores tendo uma ferramenta para troca de informações entre as universidades, sendo acessível. A comercialização da internet ocorreu apenas nos anos 80, onde teve início o surgimento de provedores de internet (ISP - *International Service Providers*<sup>24</sup>), que proporcionou a usuários comuns, terem acesso ao serviço dentro de sua casa.

Todavia, o grande responsável por alavancar exponencialmente o uso da internet, foi a criação da *World Wide Web*<sup>25</sup>, a rede mundial. O WWW nasceu no ano de 1989, sob o comando de T. Berners-Lee e R. Cailliau, no Laboratório Europeu de Física de altas energias, sediado em Genebra.

---

<sup>21</sup> Rede de Área Ampla (tradução livre)

<sup>22</sup> PAESANI, Liliane Minardi. **Direito e Internet:** Liberdade de Informação, Privacidade e Responsabilidade Civil, 7 ed. São Paulo: Atlas, 2014. e-book.

<sup>23</sup> Correio eletrônico (tradução livre)

<sup>24</sup> Provedores de Serviço Internacional (tradução livre)

<sup>25</sup> Rede Mundial de Computadores (tradução livre)



No ano de 1992, o sistema foi lançado, de modo a aumentar para 1 milhão, o número de servidores da rede.

É necessário salientar que a internet se diferencia de outros meios de comunicação por fazer uso de protocolo ou linguagem própria, denominado TCP/IP (*Transmission Control Protocol/ Internet Protocol*<sup>26</sup>), que realiza a leitura da informação propagada e faz o envio para o destino escolhido pelo usuário.

Liliane Minardi explica que essa linguagem própria é composta por hipertextos, ou seja, documentos cujo texto, imagem e sons são evidenciados de forma particular e podem ser relacionados a outros documentos. Basta um clique para ter acesso aos mais variados serviços sem necessidade de conhecer os inúmeros protocolos de acesso.<sup>27</sup>

É a partir deste formato inicial que foram sendo desenvolvidos os mais diversos tipos de serviços que passaram a ser distribuídos por meio da internet, e cada vez mais se mostram indispensáveis no cotidiano das relações sociais.

### 3.2 Relações da Internet com o Direito

O direito, sendo fruto das ciências humanas, está intrinsecamente ligado à evolução da sociedade, devendo acompanhá-la em busca de estabelecer a ordem jurídica e cumprir sua devida função social. É seu papel, através de um sistema logicamente estruturado e utilizável, os dados da vida social, isto é, as necessidades econômicas, os imperativos morais, a aspiração de justiça.<sup>28</sup>

Ao considerar que as maiores mudanças ocorrem devido a inovações, uma vez que estas introduzem no sistema situações até então inéditas e não previstas, o direito tem o dever de analisá-las de modo a sopesar riscos e benefícios para que a sociedade tenha a garantia de uma boa aplicação da tecnologia. Neste sentido, Marcel Leonardi explana:

O direito e a tecnologia não existem em um vácuo, separados e independentes entre si. Ao longo da história, certos avanços tecnológicos, a invenção da roda, a água canalizada, a imprensa, o motor a vapor, a lâmpada, a linha de produção, o telégrafo, a eletricidade, a câmera fotográfica, o telefone, o automóvel, o avião, o rádio, a televisão, a pílula

---

<sup>26</sup> Protocolo de Controle de Transmissão/ Protocolo da Internet (tradução livre)

<sup>27</sup> PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil**, 7ª Ed. São Paulo: Atlas, 2014, p. 11. e-book.

<sup>28</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1 ed. São Paulo: Saraiva, 2012, p. 150.

anticoncepcional, a energia nuclear, entre outros – forçaram o sistema jurídico a encontrar novas estruturas normativas para lidar com os riscos e as oportunidades oferecidas por tais inovações.

A tecnologia, por sua vez, pode e deve ser moldada pelo sistema jurídico. Desde a descoberta do fogo, a Humanidade estipulou normas para lidar com os problemas oriundos de suas invenções. Exemplos não faltam: limitações de acesso a tecnologias perigosas, mediante habilitação prévia ou utilização restrita a cientistas, militares e governos; diferentes níveis de responsabilidade, proporcionais ao potencial danosos de determinada tecnologia; normas especiais para o trânsito de veículos e aeronaves; diplomas legais específicos para as atividades de imprensa e de telecomunicações; teorias jurídicas a respeito dos riscos do desenvolvimento e assim por diante<sup>29</sup>

E dentre todas estas tecnologias, a internet representa um dos maiores avanços tecnológicos dos últimos tempos, com sua grande gama de aplicações e popularização por todo o globo. A internet é vista como sinônimo de evolução, praticidade, globalização, é uma evolução dinâmica e em constante aprimoramento, cada vez mais presente no cotidiano bilhões de pessoas diariamente.

Assim, Borruso, realizou a seguinte análise:

[...] o computador entrou no mundo do direito despertando os atrasos, as cautelas, a perplexidade e as desconfianças que circundam os novos fenômenos. Podem ser evidenciadas duas reações típicas dos juristas: a desconfiança, característica do mundo fechado do Direito, quando se confronta com as inovações tecnológicas; e a defesa – típica do Direito –, que se fecha e procura expelir o elemento perturbador para neutralizar as forças invasoras<sup>30</sup>

Tim Berners-Lee, um dos criadores da *World Wide Web*, traz em sua obra que em sua visão original, a web seria um apoio para ajudar as pessoas a realizarem coisas da vida real, sendo como um espelho que refletisse as relações sociais. Todavia, as pessoas vêm utilizando a internet para criar coisas que não foram construídas nem escritas fora dela, e a *Web* se torna espaço primário para muitas atividades, e dizendo que devemos ter cuidado com isso para analisar se é algo que caminha para uma sociedade justa. <sup>31</sup> É inocência estar diante de tamanhas renovações na sociedade sem se imaginar suas consequências para o direito.

A partir dos efeitos que a internet causa sobre a sociedade, as intensas mudanças que esta proporciona, gerando implicações sociais e jurídicas, que

---

<sup>29</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1 ed. São Paulo: Saraiva, 2012, p. 27.

<sup>30</sup> BORRUSO, 1978 apud PAESANI, 2008, p. 13

<sup>31</sup> BERNERS-LEE, Tim. **Weaving the Web: the original design and ultimate design of the World Wide Web by its inventor**. Nova York: HarperCollins Publishers, 2000, p. 165.

tiveram início as preocupações a respeito desta vertente. Primeiramente, este interesse começou dentro do ambiente acadêmico, onde as universidades americanas foram pioneiras criando centros de estudo a respeito do tema, tais como *Berckman Center for Internet and Society*<sup>32</sup>, da Faculdade de Harvard; Stanford Center for Internet and Society; da Faculdade de Direito da Universidade de Stanford; chegando ao Brasil com o Centro de Tecnologia e Sociedade (CTS), da Escola de Direito da fundação Getúlio Vargas do Rio de Janeiro.

Todavia, as implicações jurídicas e sociais da internet não se restringiram a serem analisadas somente dentro do meio acadêmico. Organizações não governamentais e entidades foram criadas visando o estudo desses temas, além de promover eventos como congressos, palestras e debates de forma a difundir o conhecimento aplicado nesta área.

O *Internet Governance Forum* <sup>33</sup>(IGF), foi criado em 2006 com a finalidade de proporcionar suporte para questões pertinentes à governança da Internet para a Organização das Nações Unidas, fomentando debates entre especialistas envolvendo políticas públicas na área. Há de se ressaltar que este fórum é internacional, de forma que muitos Estados participam, tendo que a segunda edição deste evento no ano de 2007, foi realizada no Brasil, e a última, no ano de 2018, realizada na França.

Defronte às discussões levantadas pelos estudos, uma das mais polêmicas, encontra-se na análise da criação de uma área do direito voltada ao estudo das implicações jurídicas decorrentes da internet.

A respeito dessa discussão, uma convenção em Chicago, no ano de 1996, levantou a discussão:

Em uma conferência sobre a "*Law of Cyberspace*", realizada na Universidade de Chicago, no ano de 1996, o juiz norte americano Frank Easterbrook observou não existir nenhum "direito ao cyberspaço" (*Cyberlaw*), do mesmo modo que não existe nenhum "direito do cavalo" (*law of the horse*). Em síntese, sustentou que a melhor maneira de aprender o direito aplicável a questões especializadas era estudar regras gerais <sup>34</sup>

---

<sup>32</sup> Centro Berckman para Internet e Sociedade (tradução livre)

<sup>33</sup> Fórum de Governo da Internet (tradução livre)

<sup>34</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1 ed. São Paulo: Saraiva, 2012, p. 32.

E diversos autores compartilham dessa mesma ideia, uma vez que entendem o cyberspaço como apenas outra mídia, que não foi capaz de criar um bem jurídico a ser tutelado, como entendem Amaro Moraes e Silva Neto <sup>35</sup>.

Em primeiro momento, esse raciocínio parece ser interessante saída para a não regulamentação de um ramo do direito especializado à internet, pois se estende a aplicação de institutos jurídicos gerais aplicando aos conflitos que então surgirem. Todavia, na prática, uma mera adequação de regras, na prática não é capaz de gerar bons resultados. Exige-se uma nova forma de interpretar o ordenamento jurídico em busca de solucionar adequadamente os problemas oriundos da internet.

Marcel Leonardi apresenta que a internet não é moda passageira e deve ser vista como um problema novo para a ciência jurídica <sup>36</sup>. Além disso, se vê a sociedade da informação como causadora de grandes impactos em mudanças em toda uma gama de negócios jurídicos diretos e indiretos através da utilização de tecnologia da informação associada à internet.

De modo geral, é inegável a influência da internet na vida humana, e como esta é irreversível, baseando-se apenas no modo de operação o qual a sociedade como um todo vem estabelecendo utilizando esta ferramenta. Atualmente, a necessidade de discussão sobre os estudos das consequências sociais e jurídicas decorrentes da internet, ainda são necessárias. Eventualmente, quaisquer sejam os ramos do direito irão enfrentar questões derivadas de relações da internet, e uma aplicação destacada destes temas passará a ser dispensável.

Conclui-se, portanto, a ideia da necessidade da preocupação do Direito com as relações derivadas da internet, pois estas são em muitos casos, inéditas dentro da sociedade, e apresentam funcionamento diferente do que o ordenamento jurídico brasileiro estabelece até então, merecendo tutela para que se tenha a efetivação de direitos dentro da sociedade da informação.

---

<sup>35</sup> MORAES, Amaro; NETO, Silva. **Falácia eletrônica**: a internet não criou um novo bem jurídico a ser tutelado. **CONJUR**. Disponível em: [https://www.conjur.com.br/2006-dez-06/internet\\_ao\\_criou\\_bem\\_juridico\\_tutelado](https://www.conjur.com.br/2006-dez-06/internet_ao_criou_bem_juridico_tutelado). Acesso em: 29 mar. 2019

<sup>36</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1 ed. São Paulo: Saraiva, 2012, p. 34.

### 3.3 A Internet e sua Regulamentação

Embora esteja muito presente na vida das pessoas em geral, existe grande dificuldade dos juristas e legisladores no que condiz à internet. A falta de análises mais profundas, ausente de discussões com a comunidade científica e acadêmica, impossibilita a criação de dispositivos de lei que realmente consigam encarar as questões jurídicas existentes nesta área.

Existe a omissão no que se refere a ultrapassagem dos mecanismos tradicionais de tutela na rede, para que melhor sejam estabelecidos. Todavia, a tutela na rede é moldada às características próprias da Internet, uma vez que seu funcionamento não consegue ser coordenado apenas com base em regras gerais.

De maneira a explanar a dificuldade de regulação da internet, primeiro, é necessário verificar seu modo de funcionamento.

A Internet foi elaborada baseada no princípio de criação de redes informáticas chamado fim-a-fim. Com isso, os equipamentos que fazem a internet funcionar, realizam tarefas simples, mas que sejam necessárias para diferentes funcionalidades, como transmissão de pacote de dados o início ao destino, enquanto as tarefas com maior complexidade ficam a cargo de aplicativos específicos, através das máquinas que acessarem a rede.

Deste modo, a complexidade e inteligência ficam a cargo das máquinas que realizam o acesso à rede em suas extremidades, enquanto a rede por si, se resguarda apenas em transmissão de dados. Um exemplo deste funcionamento se dá no abastecimento de energia elétrica, onde as tomadas somente fornecem eletricidade sem controlar quaisquer dos aparelhos que irão fazer o uso dela.

É um método que apresenta benefícios, tais como: novos aplicativos somente precisam ser conectados à rede para operarem, uma vez que são executados em computadores em uma extremidade da rede, sem alteração de computadores dentro dela; como o design é neutro, sem nenhuma aplicação específica, é um ambiente aberto para abraçar funcionalidades que não foram previstas inicialmente, gerando ampla área de oportunidades para inovações; a neutralidade da rede também impede que ela passe a priorizar uma aplicação em detrimento de outra, ou seja, se um novo aplicativo pode dominar público pertencente a outro, a rede se mantém indiferente, incapaz de qualquer atitude a respeito.

Do ponto de vista do progresso, quando os benefícios e consequências da utilização de uma tecnologia não podem ser previstos, a abstenção de regulamentação é uma forma interessante de analisar as aplicações que ela tem capacidade de ter. Diante do desenvolvimento, a incerteza a respeito de uma tecnologia é fundamental para permitir que cresça e desenvolva de diversas maneiras.

Foi com a utilização desta ideia que permitiu a utilização da rede em modo neutro, permitindo o desenvolvimento de conteúdos de formas não imaginadas à época em que foi projetada.

Entretanto, existem desvantagens nítidas, como apresentado por Marcel Leonardi:

Do ponto de vista regulatório, porém, as desvantagens do princípio *end-to-end* são igualmente evidentes. A ausência de mecanismos confiáveis de autenticação da identidade de usuários, a ampla liberdade de utilização da Internet para quaisquer fins e a possibilidade de publicação de informações em tempo real para uma audiência global, sem autorização nem controle editorial prévio de quem quer que seja, podem ser facilmente abusadas, sem que haja a correspondente responsabilidade. Por si só, a Rede não consegue discernir quais funções ou conteúdos devem ser permitidos ou proibidos, pois foi projetada dessa maneira<sup>37</sup>

Seja o princípio uma vantagem ou defeito, a ausência de um controle central é a maneira da qual a internet foi projetada.

### 3.3.1 Legislação pertinente

Quando se trata de legislação que versa a respeito do ambiente digital, nos deparamos com outro parâmetro de análise de relações sociais, políticas, econômicas, históricas, tendo estes novos tratamentos perante à sociedade.

Na legislação brasileira, um grande marco legislativo diante do direito digital encontra-se o Marco Civil da Internet (Lei N° 12.965/14), uma legislação cujo principal objetivo era de regulação das relações sociais de usuários da internet. Inicialmente porque a internet se mostra um ambiente revolucionário diante das relações, onde um simples comentário fixa-se indefinidamente em bancos de dados e servidores, e haverá o registro por tempo indeterminado, ao passo que fora dela,

---

<sup>37</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1 ed. São Paulo: Saraiva, 2012, p. 134.

por exemplo, um comentário na rua, se não realizado seu registro, se desvai naquele momento.

Todavia, o Marco Civil da Internet não atingiu os objetivos esperados, trazendo previsões principiológicas muito amplas e deixando de trazer provisões legais que realmente viessem a regulamentar o ambiente digital de acordo com as necessidades fáticas. Uma das maiores críticas versa a respeito da ideia trazida pela lei de que a tecnologia, sendo fenômeno de transformação, equaliza todos, quando em realidade, é o exato oposto, pois aqueles que a dominam são capazes de construir mecanismos os quais manipulados de acordo com seus interesses, cria barreiras e impede a conquista de direitos.

Além disso, a lei não contextualiza direitos preexistentes e que são entendidos como cabíveis a todos os cidadãos e usuários da rede, tal como o direito à privacidade, à vida privada, do acesso à informação. Há também, críticas no sentido da lei trazer uma descomedida interferência do Poder Judiciário para essas relações, mas a interferência do juízo é necessária para que a internet se desenvolva?

Acerca da interferência do Poder Judiciário, encontram-se os casos de bloqueio da rede social WhatsApp, onde juízes, ao terem ordens judiciais de fornecimento de informações negados pela empresa, simplesmente enviam ordens de bloqueio para as operadoras de telefonia de modo que atinja a todos os usuários da rede no Brasil a restrição do uso do aplicativo. A primeira decisão foi dada pela 1ª Vara Criminal de São Bernardo do Campo em dezembro de 2015, em processo de investigação de suposto tráfico de drogas, associação a organização criminosa e latrocínio. Em segundo caso, em maio de 2016, pela Vara Criminal de Lagarto (SE), houve inclusive, decretação de prisão ao vice-presidente do WhatsApp.

Em breve análise, o Poder Judiciário não se mostra efetivamente preparado para lidar com tais espécies de lide. A lei peca muito ao não estabelecer os parâmetros corretos para efetiva regulação da internet, trazendo apenas regulações universais, como a respeito da privacidade, um direito fundamental que sofre constantes alterações, uma vez que a ideia inicial deste direito certamente já se mostra ineficaz no cenário atual, com a utilização de tecnologias de informação cada vez mais desenvolvidas.

No ano de 2018 foi promulgada no Brasil a Lei de Proteção de Dados Pessoais (LGPD), sendo vista como um marco legal relevante, por tratar da proteção

de dados, envolvendo instituições privadas e públicas em qualquer tratamento que envolva o tema, incluindo tanto a pessoa jurídica como a pessoa física.

É uma legislação principiológica, que segundo Patrícia Peck, visa:

[...] a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico <sup>38</sup>

A LGPD buscou diretamente regulamentar conforme o modelo de negócios da sociedade da informação, que tem como um de seus elementares basilares, bancos de dados, que tem fluxo internacional, movimentando o mercado digital. Assim, perante a imprescindibilidade de um acordo entre os usuários, cidadãos da sociedade da informação e as instituições que manejam o tratamento de dados pessoais.

A conforme o art. 3º da lei, esta é aplicada a todos que fazem operações de tratamento de dados, podendo ser pessoa natural ou pessoa jurídica de direito público ou privado, independente do meio, país de sede ou onde estejam localizados os dados, mas necessita a presença de um dos seguintes elementos: a operação de tratamento seja realizada no Brasil; que haja o objetivo de fornecimento de bens ou serviços ou tratamento de dados para indivíduos localizados no território nacional; ou os dados tenham sido coletados no Brasil.

Ao analisar o dispositivo, verifica-se que a lei não se importa com o local de residência do titular e a nacionalidade dos dados também se mostra indiferente. Mas é preciso salientar que a lei não se aplica à pessoa física que tenha fins exclusivamente pessoais e não econômicos. Além disso, verifica-se a extraterritorialidade da LGPD, uma vez que os dados colhidos no Brasil, mesmo tratados no exterior, terão ainda que obedecer à legislação nacional.

Por fim, após esta breve análise, mostra-se que a LGPD buscou discorrer sobre os dados pessoais reconhecendo o seu valor dentro da estrutura de mercado que se desenvolveu com a sociedade da informação, sendo realmente uma moeda entre os usuários para ter acesso a bens e serviços.

No âmbito internacional, a proteção de dados há muito tempo, como se verifica a presença de positivação do tema nas Cartas Constitucionais de países

---

<sup>38</sup> PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**: comentários à Lei nº 13.709/18 (LGPD). São Paulo: Saraiva Educação, 2018, p. 31.



como Portugal, na Constituição da República Portuguesa, em seu artigo 35, desde o ano de 1976, e a Espanha, na Constituição Espanhola, em seu artigo 18.4, desde o ano de 1978.

Portugal foi pioneira na previsão deste tema historicamente, pois no ano de 1973, com a lei nº 2/73, instituiu o registro nacional de identificação. Após isto, em sua lei fundamental dispôs sobre os direitos de seus cidadãos acerca da proteção de dados em seu artigo 35, que expõe o seguinte:

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expreso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.<sup>39</sup>

Estes dispositivos legais demonstram a visão que o parlamento português já possuía acerca dos dados pessoais, demonstrando preocupação quanto à sua regulamentação e incluindo em sua proteção inclusive dados que não estivessem arquivados em meio eletrônico.

No que condiz à União Europeia, a previsão legal acerca do tema também se mostra prevista em Tratados, como o Tratado sobre o Funcionamento da União Europeia, que traz em seu artigo 16 o direito das pessoas à proteção dos dados que lhe dizem respeito; na Carta dos Direitos Fundamentais da União Europeia tal previsão é reproduzida, e também a previsão na Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais.

Há de se salientar a Convenção do Conselho da Europa para a Proteção dos Indivíduos face ao Tratamento Automático de dados pessoais, uma convenção datada em 28 de janeiro de 1981, que inclusive traz em seu texto

<sup>39</sup> PORTUGAL. **Constituição da República Portuguesa**. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em 23 out. 2019.

conceitos como o que seriam dados de carácter pessoal, tratamento automatizado e dados sensíveis, em seus respectivos artigos 2º e 6º, respectivamente:

Art. 2º: a) «Dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados»);

c) «Tratamento automatizado» compreende as seguintes operações, efectuadas, no todo ou em parte, com a ajuda de processos automatizados: registo de dados, aplicação a esses dados de operações lógicas e ou aritméticas, bem como a sua modificação, supressão, extracção ou difusão; Os dados de carácter pessoal que revelem a origem racial, as opiniões políticas, as convicções religiosas ou outras, bem como os dados de carácter pessoal relativos à saúde ou à vida sexual, só poderão ser objecto de tratamento automatizado desde que o direito interno preveja garantias adequadas. O mesmo vale para os dados de carácter pessoal relativos a condenações penais <sup>40</sup>

Uma grande novidade legislativa no continente europeu foi, no ano de 2018, a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation* ou GDPR), que veio substituir a Diretiva 95/46/EC, da década de 90, trazendo previsões acerca de conceitos inexistentes no período, como big data, aplicativos, redes sociais, publicidade direcionada, marketing comportamental, computação em nuvem, e outros. Para melhor apresentar o que este regulamento buscou, tem-se que:

Diferentemente da Diretiva – que estabelecia diretrizes para que cada Estado-Membro da União Europeia adotasse sua própria lei de proteção de dados –, o GDPR foi desenvolvido visando à harmonização das leis de proteção de dados dos países da União Europeia, sendo vinculativo e aplicável a todos os Estados-Membros. Por outro lado, o GDPR também garante aos Estados-Membros certa margem de autonomia para elaborarem disposições mais específicas para adaptar a aplicação das regras previstas no Regulamento.

Um dos principais aspectos do GDPR é a preocupação em proteger a privacidade das pessoas que se encontram no território da União Europeia. Em um ambiente de globalização e economia baseada na internet cada vez mais dependente de dados para se sustentar (*data driven economy*). O ambiente de negócios da internet traz a peculiaridade de mitigar as fronteiras físicas convencionais, produzindo grandes vantagens para a comunicação e comércio eletrônico. Entretanto, a inexistência de fronteiras do mundo digital também apresenta um grande desafio quando se trata da aplicabilidade de normas fora de uma jurisdição.<sup>41</sup>

<sup>40</sup> PORTUGAL. **Convenção 108 Para A Protecção Das Pessoas Relativamente Ao Tratamento Automatizado De Dados De Carácter Pessoal**. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 21 abril 2019.

<sup>41</sup> FERREIRA, Ricardo Barretto, et al. **Site Migalhas**. Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia. <https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao>. Acesso em 22 de abril de 2019

Com base na análise da legislação existente acerca das relações digitais, em especial no que condiz à proteção de dados, verifica-se que o Brasil, ao longo de sua história, permaneceu alheio à regulamentação do tema, algo que aconteceu apenas em 2012, com o Marco Civil da Internet, legislação que se mostrou pouco eficaz devido à falta de técnica e visão da lei, e apenas em agosto de 2018, foi publicada a Lei Geral de Proteção de Dados Pessoais, que apresentou dezoito meses para que a lei possa produzir efeitos em sua nível completo, inclusive em nível internacional, com a aplicação de sanções. Todavia, com o constante crescimento e aumento de relevância jurídica no que concerne à temática, o Brasil não pode mais manter-se alheio ao que diz respeito à proteção de dados, e assim, mudanças deverão ocorrer neste sentido.

## 4 INTERESSES DIFUSOS

Neste capítulo, serão explanados os interesses e direitos difusos de maior essencialidade à compreensão dos direitos do cidadão perante à estrutura do direito digital, de forma a efetivar o seu cumprimento, ainda que de forma não convencional ao direito.

### 4.1. Direito à Privacidade

A doutrina brasileira utiliza uma gama de termos distintos para remeter-se à privacidade, tratando em direito à vida privada, sigilo, intimidade da vida privada, entre outros.

A Constituição Federal de 1988 não faz uso da expressão privacidade, e em seu art. 5º, inciso X, declara a invioláveis: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.<sup>42</sup>

O Código Civil de 2002 também é omissivo em relação à expressão direito à privacidade, apenas trazendo em seu Art. 21 que: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.<sup>43</sup>

A expressão “privacidade” não possui no ordenamento jurídico brasileiro, um conceito único, e sim, utilizado de forma abrangente e esparsa para referir-se a direitos ligados à confidencialidade de informações pessoais.

Todavia, da mesma forma que as expressões que trazem conceitos jurídicos indeterminados, como dignidade da pessoa humana, a privacidade parece abarcar tudo que envolve o tema, e ao mesmo tempo, ser um conceito vazio por si só.

A ausência de um consenso a respeito do que se trata a privacidade cria situações de conflito diante de casos práticos e definição de políticas públicas, e diante da situação fática, pode ocorrer a inviabilização da tutela, especialmente quando existe a necessidade do sopesamento diante de outros interesses, tais como

---

<sup>42</sup> BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado, 1988.

<sup>43</sup> BRASIL, Lei n. 10.406 de 10 de janeiro de 2002. **Institui o Código Civil**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/L10406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm). Acesso em 24 de abril 2019.

a liberdade de manifestação de pensamento, a segurança pública e a eficiência de transações comerciais.<sup>44</sup>

Embora haja diversos conflitos na doutrina em relação ao que de fato pode ser conceituado como privacidade, dentro do mundo jurídico, uma das teorias mais difundidas acerca da privacidade foi através do artigo “*The right to privacy*”<sup>45</sup>, que trouxe a expressão “*the right to be let alone*”<sup>46</sup>, elaborado por Samuel D. Warren e Louis D. Brandeis. Neste aspecto, Alessandro Hirata explana o seguinte:

Ainda que bastante vaga, essa primeira concepção de privacidade deve ser interpretada como sendo o “direito de ser deixado só”, que remete à não interferência pelo Estado na vida do indivíduo. Todavia, deve-se entender a privacidade não apenas como a não interferência do Estado na vida do indivíduo, mas também como o poder de se reivindicar ao Estado a tutela dessa privacidade, protegendo o indivíduo de terceiros.

Na sociedade contemporânea, porém, a noção de privacidade extravasa os conceitos de isolamento ou tranquilidade. O “*right to be let alone*” revela-se insuficiente em uma sociedade em que os meios de violação da privacidade caminham paralelamente aos diversos e importantes avanços tecnológicos

<sup>47</sup>

Este conceito foi escrito em 1890, onde foram observados pelos autores, os instrumentos que, à sua época, representavam possíveis ameaças à privacidade. O fato ensejador da observação aplicado, faz referências a fotografias instantâneas e a indústria dos jornais, que adentraram ao ambiente inviolável da vida doméstica e privada.

Para Warren e Brandeis, a ideia da privacidade é que esta deveria ser inviolável, onde não se objetiva auferir indenização como consequência de publicação indesejada, mas na busca de poder para impedir que a publicação sequer chegasse a ser publicada. De modo que para eles, a ideia do direito de ser deixado só, é um direito de personalidade, um direito geral trabalhando com a concepção de imunização do cidadão.

Essa concepção influenciou o conceito de privacidade não só nos Estados Unidos, mas em todo o mundo. Todavia, é uma percepção vaga que não é capaz de definir o que está inserido em seu plano de proteção.

<sup>44</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1 ed. São Paulo: Saraiva, 2012, p. 47.

<sup>45</sup> Direito de privacidade (tradução livre)

<sup>46</sup> Direito de ser deixado só (tradução livre)

<sup>47</sup> HIRATA, Alessandro. **Enciclopédia Jurídica**. Direito à privacidade. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade>. Acesso em 30 mar. 2019.

Uma segunda teoria, trata da privacidade como resguardo contra interferências alheias. É o direito do indivíduo viver com um grau mínimo de interferências externas. Não se trata aqui, do isolamento social, mas sim do sujeito ser capaz de controlar o que se refira a si próprio da ciência de outrem.

Entende-se, portanto, como uma atividade de escolha do indivíduo poder selecionar informações que deseja ou não que sejam do conhecimento público, para que desta forma, proteger aquilo que almeja manter sob reserva.

Outra corrente trata o direito à privacidade como segredo ou sigilo de algumas informações do indivíduo, mas não é um resguardo para interferências de terceiros. Aqui, se aplica por exemplo, o sigilo profissional, onde não se pode liberar o segredo ao qual teve conhecimento por meio de dever profissional de agir.

Por fim, uma das correntes mais relevantes em relação à privacidade, é o controle sobre informações e dados pessoais. Neste aspecto, Marcel Leonardi traz a definição de Alan Westin para esta teoria: “para esta corrente, a privacidade é a reivindicação de indivíduos, grupos ou instituições de determinar por si próprios quando, como e em que extensão informações a seu respeito são comunicadas a terceiros. 48

Esta teoria não encara a privacidade da mesma forma que as demais, porque não trata apenas da ausência do conhecimento de terceiros a fatos da vida privada somente, e sim a entende como um poder de controle exercido sobre quaisquer informações e dados pessoas que a ele pertençam.

De acordo com José Matos Pereira, a privacidade significa o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem isso poder ser legalmente sujeito. 49

A proteção aos dados pessoais possui muito destaque no que condiz ao direito à privacidade. A informação é um bem jurídico reconhecido, de inestimável valor econômico, onde os Estados que possuem este bem em maior quantidade, tem os resultados refletidos em seu alto poder, onde a economia da informação se mostra mais evidente.

---

<sup>48</sup> LEONARDI, Marcel. **Tutela e privacidade na internet**. 1 ed. São Paulo: Saraiva, 2012, p. 67.

<sup>49</sup> PEREIRA, José Matos. **Direito de Informação**. Lisboa: Associação Portuguesa de Informática, 1980, p.15

#### 4.1.1 Interpretações acerca do direito à privacidade

No filme “Inimigo do Estado”, dirigido por Tony Scott, um dos personagens menciona a seguinte fala: “a única privacidade que você tem está na sua cabeça. Talvez nem mesmo lá.”<sup>50</sup>

Freud, realizando pesquisas acerca do subconsciente, constatou que o “eu” não está mais no controle. E conforme diz Stefano Rodotá, atualmente, podemos sustentar com segurança que a privacidade mental, a mais íntima esfera, está sob ameaça, violando a dimensão mais reclusa de uma pessoa.<sup>51</sup>

Na realidade atual, as definições de privacidade como vem sendo utilizadas não se mostram eficientes do modo que somente se refere à uma forma do indivíduo se resguardar da sociedade, como o direito de ser deixado só, sendo concepções individualistas, que diante das novas formas de coleta e tratamento de informações, são situações divergentes.

A justificativa para isto se encontra na estrutura fundamental que o direito à privacidade possui, onde a primeira geração de leis de proteção de dados (no mundo), tinha como objetivo tutelar as preocupações a respeito de violações da intimidade individual que a tecnologia poderia trazer. A partir de então existe prioridade dos conflitos jurídicos que versem sobre o tema de serem analisados sob este parâmetro.

Hoje, existem inúmeras formas de coleta de dados, sejam por instituições públicas ou privadas, que se mostram fora do alcance do indivíduo, o qual não exerce controle algum, e a economia da informação vem se fortalecendo cada vez mais com a monetização dos dados pessoais.

A regulação de coleta e circulação de informações é vista de formas diferentes. Uma delas é que regulamentações que restrinjam a coleta e circulação de informações somente são possíveis em períodos de estabilidade. Caso contrário, em períodos de instabilidade social, cresce a necessidade por informações, onde se torna crucial a conexão entre inúmeros bancos de dados para enfrentar situações emergenciais, independente da área em que ocorra o conflito.

---

<sup>50</sup> **INIMIGO DO ESTADO**. Direção de Tony Scott. Estados Unidos: Jerry Bruckheimer Films, Scott Free Productions, 1998.

<sup>51</sup> RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 14.

Nos Estados Unidos, houve os defensores da “*deregulation*”<sup>52</sup>, que foi um movimento de resistência contra intervenções legislativas, em que seus principais defensores representavam a área industrial. Atualmente, ainda ressurgem as ilusões de que as novas tecnologias possam ser auto reguladoras, retornando ao patamar existente inicialmente. Propõem ainda, que deve ser deixada toda a regulação ao mercado de modo integral, inclusive no que diz respeito à privacidade.

A *deregulation* tem forte estímulo para retornar às regras de mercado também em ambientes governamentais e científicos. Nos Estados Unidos, por sua relevante influência nesta corrente, o presidente da *Federal Communications Commission* (FCC)<sup>53</sup>, no ano de 1982, declarou ao Congresso que os problemas de “*cable privacy*”<sup>54</sup> necessitavam de intervenção federal. Além disso, sugeriu ao governo federal que deveria confiar a proteção da privacidade apenas às regras de mercado. E assim, expõe Rodotá que a privacidade receberia, assim, uma cotação de mercado e poderia ser garantida como serviço pago somente a quem dela efetivamente tivesse necessidade.<sup>55</sup>

Essa perspectiva diante da privacidade a enxerga como um objeto como qualquer outro tutelado pelas transações comerciais, como uma troca de propriedade no mercado de direitos. A principal discussão que se extrai dessa corrente é a ideia de direitos decorrentes da privacidade pode ser restrita e limitada sob ótica exclusivamente patrimonial, como um bem a ser mantido ou vendido.

A partir do crescimento de fornecimento de serviços de mídia interativa, o fornecimento de informações o acompanhou, criando grande dependência entre eles, e ao invés de evoluírem, houve a falsa ideia da desnecessidade de privacidade e a efetiva proteção de dados.

O usuário dos serviços telemáticos encontra-se em situação díspar com os fornecedores de tais produtos, e que não cabe dizer que existe o livre consentimento do consumidor no que se refere à sua privacidade.

Essas análises não pretendem trazer à tona a necessidade de intensa interferência legislativa ou não neste aspecto, mas sim demonstrar como existe grande desproporcionalidade entre o poder exercido por ambas as partes: o

---

<sup>52</sup> Desregulamentação (tradução livre)

<sup>53</sup> Comissão Federal de Comunicações (tradução livre)

<sup>54</sup> Privacidade de cabo (tradução livre)

<sup>55</sup> RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 52.



fornecedor e o usuário, embora certa intervenção legislativa neste aspecto se mostra sim necessária para nortear corretamente a direção cuja as regras de mercado devem seguir.

Considera-se ainda, que o tema da privacidade envolve diversas dimensões de garantias de direitos fundamentais e direitos civis, em prol de uma democracia, onde seus interesses não podem ser reduzidos à mera esfera individual e irreduzível à lógica exclusivamente proprietária.

A matéria da proteção de dados em alguns países, já alcançou o auge da hierarquia de fontes jurídicas, como o reconhecimento em nível constitucional, como nas Constituições da Espanha e Portugal, e discutida na Convenção do Conselho Europeu, por exemplo.

Diante dessas ideias, Stefano Rodotà apresenta posicionamento muito interessante no que condiz à regulamentação da privacidade e a proteção de dados:

O problema, na verdade, não se coloca em termos de “regulação, sim ou não”, de direito ou não direito. A verdadeira questão diz respeito à possibilidade de atribuir um valor orientador, para o futuro, a categorias e conceitos que, como um dos contratantes hipossuficientes ou da privacidade, foram elaborados para situações em que a informação como um recurso ainda não ocupava posição central. Trata-se, portanto, de criar instituições adequadas à nova situação (afinal, de que forma o direito moderno, filho da revolução industrial, substituiu o feudal?), no âmbito das quais cabe responder também aos interesses e às exigências que, por costume ou falta de imaginação, continuamos a chamar pelos nomes antigos<sup>56</sup>

A nova era do Direito não condiz com hipótese de adequação da estrutura já existente para aplicação nas novas situações jurídicas que vem ocorrendo, e sim uma transformação de valores exigida pela sociedade da informação e realize nova análise de princípios fundamentais para que se mantenha aquilo que se denomina de liberdade e democracia.

## 4.2 Direito à Informação

O direito à informação costuma ser analisado sob a ótica de duas vertentes: o direito de informar e de ser informado. Englobando em sua primeira categoria, o acesso aos meios de informação em igualdade de condições, o direito

---

<sup>56</sup> RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 58.

de expressar seu pensamento e de efetivamente informar. Já a segunda vertente inclui uma ótica passiva do direito, de receber a informação.

Constitui, portanto, um único direito, mas que devido à sua divisão para fins de melhor aplicação, deve conter ambas as condições em equilíbrio para efetivar a ideia do estado democrático de direito trazido pela Constituição Federal.

A sociedade da informação trouxe consigo diversos instrumentos que implementaram mecanismos facilitadores de acesso à informação, todavia, este se dá através de sistemas articulados, os quais foram reconhecidos por legislações em nível constitucional em diversos países do mundo.

A amplitude da liberdade de informação apresenta embasamento na Constituição Federal, especialmente no art. 5º, inciso IX e art. 220, que tratam especialmente da informação.<sup>57</sup>

Pois bem, os meios de comunicação e informação não foram estabelecidos por si só, mas sim, estruturados conforme a previsão constitucional deste direito para sua efetivação. Neste sentido, Liliana Paesani expõe:

A liberdade informática, ou seja, a utilização de instrumentos informáticos para informar e para informar-se, não é uma consequência natural da configuração da Internet, é uma decorrência direta da liberdade de informação que se fundamenta em preceito constitucional<sup>58</sup>

Desta forma, é possível extrair a relevância de um direito significativo de tal forma que o sistema adequa seu funcionamento a ele, e não o contrário, estando cada vez mais presente na sociedade atual, cuja economia se baseia cada vez mais no fluxo informacional, das mais variadas formas.

### 4.3 Direito à Proteção de Dados Pessoais

Um dado é a matéria prima bruta da informação, cuja conversão em conhecimento benéfico não é automática. Os dados são materiais que, quando

---

<sup>57</sup> Art. 5º. IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

<sup>58</sup> PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil**, 7. ed. São Paulo: Atlas, 2014, p. 6. *e-book*.

transformados, processados e organizados, podem ser transformados e deles, extraídas informações que se convertem em conhecimento.

Estas fontes de informação encontram-se presentes em inúmeros locais, sendo disponibilizados pelo próprio usuário, como em redes sociais, até cadastros públicos e privados, aos quais, o acesso pode ou não ser restrito. É a partir de então, que surge a necessidade de proteção dos mesmos, para proteger essencialmente o detentor destes dados, e especialmente, sua privacidade.

No exemplo apresentado acerca da multinacional Zara é visível esta funcionalidade. Coletar dados sem finalidade alguma, aparentemente não apresenta significado algum, mas quando organizados com o objetivo de se analisar estatísticas de vendas para montagem de estratégias de marketing de novos produtos, é o momento de obtenção de informação relevante.

Os equipamentos eletrônicos quando conectados à internet, recebem o nome de clientes e servidores. Os clientes são aqueles que buscam acessar algum site ou aplicativo, os usuários de maneira geral. Já os servidores podem ser comparados a bibliotecas virtuais, armazenando os aplicativos ou páginas da web, de forma que quando um cliente acessa uma página, é baixada uma cópia do servidor para a sua máquina, que será disposto em seu browser.

Os *browsers*<sup>59</sup> nada mais são que uma espécie de programa que permite a navegação na internet, sendo uma forma de acesso ao que está disponível na rede, sendo muito comuns no Brasil o Google Chrome, Mozilla Firefox e Safari.

Um banco de dados envolve o processamento de dados de forma dinâmica, pois os dados entram (*input*), são processados, dali saem informações. É procedimento que requer administração, uma vez que por si só, são estáticos e não se convertem em conhecimento algum, seja manual ou automatizado.

As tecnologias da informação foram essenciais para este processo, especialmente ao se tratar dos softwares, os quais automatizaram a gestão de banco de dados modificando a ordem a quantitativa e qualitativa do processamento desses dados.

---

<sup>59</sup> Navegadores (tradução livre)

Neste sentido, Peter Rob explica a definição de banco de dados:

É um conjunto de programas que gerenciam a estrutura dos bancos de dados e controlam o acesso aos dados armazenados. Até certo ponto, o banco de dados se assemelha a um arquivo eletrônico com conteúdo bem organizado com a ajuda de um software poderoso, conhecido como sistema de gerenciamento de bancos de dados<sup>60</sup>

A seguir, demonstra papel dos softwares para aplicação deles:

Softwares consiste nos programas de computador que governam a operação de um computador. Esses programas permitem que um computador processe a folha de pagamentos, envie contas aos clientes e proporcione ao gerente informações para ampliar os lucros, reduzir os custos e oferecer melhores serviços aos clientes. Existem dois tipos básicos de softwares: softwares de sistemas, como Windows XP, que controla as operações básicas do computador, como a inicialização e impressões, e software de aplicação, como o Office XP, que permite a execução de tarefas específicas, como o processamento de textos e tabulação de números<sup>61</sup>

Perante os softwares, fala-se em automatização parcial, uma vez que eles mantiveram o ser humano com o papel de alimentação do banco de dados, o qual armazena todas as informações e as gerencia. É partir de então que se emitem os conhecimentos necessários para quem utiliza da ferramenta.

Um exemplo prático e simples, corresponde às empresas que inserem o nome do cliente, sendo esse o principal referencial para acessar os demais dados, sendo a entidade, e depois a complementação de outros dados, como valor do serviço prestado a ele, seu telefone e endereço, chamados atributos. Assim, por meio do acesso a essas informações dentro do banco de dados da empresa, os administradores desta poderão ter o controle de clientes, saldos, faturas de cobrança, sendo denominado banco de dados operacional.

É interessante salientar os *data warehouses*, que funcionam da mesma forma do banco de dados, todavia, direcionados para tomadas de decisão. A utilização desse sistema de controle de dados possibilita, ao analisar os dados de cada cliente, seu devido perfil, faz com que a empresa seja capaz de direcionar a cada um, a abordagem mais atraente a cada perfil, dentro do meio eletrônico, o envio de e-mails ou a produção de vídeos, a depender da análise dos dados.

---

<sup>60</sup> ROB, Peter. **Sistemas de Bancos de Dados**: projeto e implementação. Trad. All Tasks. São Paulo: Cengage Learning, 2011, p. 6.

<sup>61</sup> ROB, op. cit., p. 6.

Neste formato, é destacada a possibilidade de armazenamento de inúmeros dados dos usuários da internet, que são coletados e a partir de uma gerência apropriada, são analisadas as formas de publicidade direcionada que serão encaminhadas a cada usuário. Consiste em fato relevante na atualidade e que permite a concretização da publicidade comportamental.

O banco de dados não existe por si só, passando por processo de coleta, estruturação, identificação, análise, até a conversão do dado em informação, que por fim, pode se transformar em conhecimento. Não apenas um agrupamento de informações, mas informações que serão manipuladas com a finalidade de serem extraídas e com elas se tomem decisões importantes.

É a partir deste banco de dados que o ser humano manipula da forma desejada para alcançar seus objetivos finais em conformidade com a atividade que exerce, de maneira que os dados de cada indivíduo sob o controle deste banco, podem ser utilizados de diversas maneiras não autorizadas pelos seus proprietários, os quais dificilmente tomam ciência dos usos que tais informações cedidas irão obter, mas sofrem com as consequências de sua utilização.

## **5 A RELEVÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS E SUA APLICAÇÃO PRÁTICA**

Como apresentado no tópico anterior, a privacidade e a proteção de dados se mostram temas de extrema importância no cenário atual, de intensas mudanças de paradigmas, desde a mudança comportamental da sociedade à troca de ideais da estrutura comunicacional do mundo.

Atividades que antes demandavam uma quantidade de tempo muito significativa, hoje podem ser realizadas a um toque em uma tela, informações que demandavam trabalhos manuais para serem computadas, podem ser analisadas por softwares e armazenadas por banco de dados, acessíveis a qualquer momento, e que realizam tarefas em conformidade com os desejos de quem os manipula.

A privacidade, um direito fundamental angariado ao ordenamento jurídico brasileiro em sua carta magna, com suas dificuldades de conceituação, haja vista ser uma ideia vaga e adaptável à casuística do momento em que se aplica, já não se mostra tão somente suficiente para atender às necessidades da proteção dos dados pessoais.

Os dados pessoais, com o advento de novos mecanismos de controle, passam a ser de relevante interesse a quem os utiliza, e a aqueles que cedem seus dados. Apesar de sua íntima ligação com o direito à privacidade, especialmente no que condiz à sua justificativa, de proteção a esfera da vida do cidadão a qual este tem o direito de abster do conhecimento público, já não se mostra suficiente no que se refere ao direito digital, a proteção de dados pessoais, pois estes já não se limitam a simples fato que não se deseja compartilhar, mas sim, informações relevantes a respeito do sujeito que os detém.

A proteção de dados pessoais está estritamente ligada com a tutela ao direito constitucionalmente previsto, a privacidade, o qual foi abarcado de diferentes formas, em busca de alcançar diferentes patamares da vida do sujeito de direito, nos quais é possível verificar a proteção de dados como um deles.

Então, a distinção entre direito à intimidade, à vida privada e familiar e direito à proteção de dados pessoais se mostra essencial a este estudo, iniciando pelo direito à intimidade.

O direito à intimidade, à vida privada e familiar e o direito à proteção de dados são institutos os quais não se confundem, embora aparentemente ambos pareçam tratar da esfera mais íntima do ser humano.

A primeira consiste em situação onde se veda a interferência de terceiros na vida privada e familiar. A vida privada envolve todas as informações que a pessoa tem a capacidade de escolha entre compartilhar ou não com o público, sendo um tipo de proteção negativa, pois seus objetos são estáticos, em caráter individualista e somente isto.

Já a proteção de dados se apresenta de forma mais dinâmica, pois trata de regras e mecanismos acerca de processamento de dados e a legitimidade para tomada de decisões, sendo uma proteção dinâmica, pois é necessário seguir os dados para que se efetive.

O direito à privacidade, conforme Bruno Bioni expõe, vem sendo manipulado diante de duas perspectivas diferentes:

O direito à privacidade tem sido historicamente articulado com base na dicotomia entre as esferas pública e privada. Sempre esteve em perspectiva a demarcação de atividades que deveriam ser desempenhadas privativamente ou em público vis-à-vis<sup>62</sup>

É desta forma que se entende a residência como a esfera particular do indivíduo, onde seria o símbolo da faculdade de afastar-se da sociedade, o direito de recolher-se para poder refletir sobre suas próprias ideias, podendo, somente neste momento de fuga social, desenvolver ao máximo sua subjetividade para após, ter possibilidade de expor-se corretamente à sociedade.

Há também, a chamada teoria das esferas, a qual explica a existência de maiores ou menores graus de intimidade da informação, de acordo com quais pessoas aquele que detém a informação opta por compartilhar, delimitando áreas de sua vida particular em vários níveis, conforme sua vontade.

Assim, mesmo as informações compartilhadas, se isto for feito entre amigos, ainda pertence à esfera privada, pois a propagação desse dado não será feita indiscriminadamente por aqueles que a receberam. É neste âmbito que o direito à privacidade trabalha em grande parte, em dividir aquilo que cabe escolha da pessoa em manter privado ou aberto ao conhecimento de todos, essencialmente na

---

<sup>62</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2018, p. 92.

ideia que o direito à privacidade é uma liberdade negativa, que consiste na ideia de terceiros não poderem interferir na vida privada, intimidade de outrem.

É diante deste aspecto que o direito à privacidade se mostra como estrutura basilar para o advento do direito à proteção de dados, todavia, sua estrutura estática não é capaz de suprir as necessidades que vem surgindo.

A proximidade da proteção de dados com o direito à privacidade é esclarecida por Bruno Bioni, que trata claramente das razões que a separa como um direito autônomo, e não somente uma dimensão ou evolução:

O direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade. Pelo contrário, demanda-se uma correspondente ampliação normativa que clareie e não empole a sua tutela.

A própria intelecção do objeto jurídico em questão não é conduzida pela dicotomia entre público e privado. Toda a sua construção é balizada pelo conceito de dado pessoa, o que pode ser vis-à-vis uma informação pública ou privada.<sup>63</sup>

A questão chave encontra-se no fato de que a proteção de dados não encontra limite dentro de esferas públicas ou privadas, sendo suficiente que a informação esteja vinculada a um indivíduo para que possa emanar efeitos.

Cabe enfatizar, conforme Bruno Bioni expõe, o tratamento de dados se mostra cada vez uma atividade de maior impacto na vida das pessoas, em questão de estarem sujeitas a decisões automatizadas:

Além disso, observa-se que cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas estão submetidas a processos de decisões automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade<sup>64</sup>

Portanto, o direito à proteção de dados pessoais, embora embasado no direito à privacidade, não pode permanecer vinculado a ele, a possibilidade de ele impedir o natural desenvolvimento da proteção de dados, corrompendo a tutela deste novo direito da personalidade.

---

<sup>63</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2018, p. 98.

<sup>64</sup> BIONI, op. cit., p. 99.



A era da informação é dinâmica, sendo os dados pessoais um prolongamento da personalidade da pessoa, tendo efeitos diretos e indiretos apenas com o controle e valor que se atribui a eles, especialmente com a monetização dos dados pessoais.

A sociedade da informação é movida por dados, e cada dado inerente a um usuário, por exemplo, dentro do sistema, é a sua junção que causa uma projeção sua dentro do mundo virtual, e claro, com consequências no mundo natural.

E neste movimento, um simples ato de um indivíduo gera dados, independentemente de onde tenha sido acessado. Isso não apenas oriundo de grandes empresas, mas cada usuário individualmente da mesma forma, uma vez que todos possuem um perfil, o qual é complementado com suas informações de mensagens, ligações, cartões de crédito, histórico de pesquisas, por exemplo.

E diante deste conjunto de dados armazenados, eles podem ser utilizados com diversas finalidades, seja para fins de publicidade, como forma de mapear as preferências dos usuários, e assim direcionar qualquer tipo de mercado que possa fazer uso deles. Acerca dessas informações, Ronaldo Lemos expõe o seguinte:

A quantidade de informações digitais é inesgotável: toda interação eletrônica, toda operação bancária e de crédito e cada simples assinatura de uma revista ficarão digitalmente gravados e ligados a indivíduos específicos, havendo notável risco de violação do sigilo desses dados para finalidades várias, inclusive ilícitas, ainda que inúmeros usuários da rede não tenham ciência do perigoso rastro que deixam a cada acesso. Tal registro de dados fica armazenado através de cookies, que servem para guardar diversas informações sobre preferências do utente, quando foi realizado o último acesso à página que instalou o respectivo cookie, senha de acesso ao site, entre outras<sup>65</sup>

Pode se dizer que se classifica como um novo tipo de identidade, em que as informações são como dossiês individuais e que devem estar corretos para que projetem corretamente a identidade de seu titular. A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) traz como um de seus princípios em seu artigo 6º, inciso V, exatamente esta previsão, preconizando a destinação do dado ao seu escolhido fim, e que estejam somente informações verdadeiras.

---

<sup>65</sup> LEMOS, Ronaldo et al. **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 739-740.

Neste sentido, serão apresentadas as ideias que se referem à interferência nos dados pessoais no sistema atual e justificada sua relevância jurídica.

### **5.1 No que Consistem os Dados Pessoais**

A tecnologia facilita imensamente o fornecimento de informações que podem ser utilizados contra o seu sujeito, isto, devido ao fato que, por ser um ambiente digital, os usuários parecem esquecer que a internet também é um ambiente tutelado por lei.

É preciso constar que a supervisão desses dados não é limitada aos seus sujeitos, e muitas vezes é concedida a terceiros, a autoridades, como um órgão público que maneje essas informações, há toda uma redistribuição de poderes sociais e legais, sendo a última parada da evolução do direito à privacidade, em sua escala mais complexa e dinâmica, que envolve desde o direito de ser deixado em paz, a mudança do controle no âmbito privado de cada indivíduo e como o domínio de informações próprias e de terceiros será convencionado.

A coleta de dados tornou-se uma prática convencional e comum, pois existem inúmeras formas de serem realizados, como redes sociais, cadastros em geral, compras feitas online. Nestes ambientes, os indivíduos geralmente inserem todos os dados que lhes são pedidos, independente de realizar a leitura dos termos de uso, por exemplo, simplesmente os aceitando.

E desta forma os usuários já possuem suas informações na rede, porque ao menos o mínimo, ele mesmo prestou-se a inserir, de modo que estejam à disposição de empresas e qualquer um que tenha permissão para acessar, de maneira geral. Todavia, também é necessário considerar que os sistemas não são absolutos, e podem ser invadidos, de forma que todos os dados coletados sejam utilizados por sujeitos desconhecidos, onde cada clique do usuário, deixou suas pegadas na rede.

Neste diapasão, é necessário salientar a distinção entre cadastro de consumidores e banco de dados de consumidores.

O primeiro mostra-se como informações que o fornecedor mantém, inicialmente, para uso próprio, proporcionando a ele uma análise na medida em que

conhece seus consumidores, proporcionando a ele ter um canal de comunicação com eles, direcionando suas ações de marketing, sem excluir a possibilidade destes cadastros serem transmitidos a terceiros.

Os bancos de dados de consumidores apresentam um horizonte maior que o anterior, sendo arquivos alimentados por empresas especializadas, com o objetivo de conceder aos fornecedores, informações a respeito de seus consumidores, muito além dos dados básicos que o fornecedor possui em seu cadastro, aqui faz-se uma análise mais profunda de cada um de forma objetiva.

## **5.2 A Estratégia Mercadológica dos Negócios Online: o Modelo Freemium**

O modelo tradicional de negócios é baseado na relação em que o consumidor deve realizar o pagamento do produto ou serviço que utilize. O crescimento das tecnologias de informação tornou possível um novo modelo de negócios, onde os negócios online podem oferecer seus serviços sem necessidade de pagamento inicial, e muitos são capazes de continuar fornecendo a prestação sem nunca haver o pagamento direto.

Mas isto não significa que os negócios online não requeiram investimentos, tanto quanto negócios offline, e ainda que inicialmente possa suportar usuários sem o efetivo pagamento, o rendimento permanece como requisito essencial de todos os mercados.

Todavia, no âmbito digital, os usuários estão acostumados a não pagar pelos serviços que consomem, e muito dificilmente irão começar a realizar pagamento por algo que já possuíam de forma gratuita desde o começo. A imposição de um pagamento tende a gerar migração de usuários para outras plataformas que ofereçam serviço similar.

Diante destas circunstâncias, o novo modelo de negócios também requer de novos métodos para rentabilizar seus serviços.

O serviço gratuito normalmente é um modelo que costuma atrair usuários para que façam o uso da plataforma, por exemplo, e gerem um valor não monetário, que poderá ser monetizado pela empresa. A monetização pode ser realizada de muitas formas, como Chris Anderson exemplifica trazendo o “freemium”:

Isn't it just the free sample model found everywhere from perfume counters to street corners? Yes, but with a pretty significant twist. The traditional free sample is the promotional candy bar handout or the diapers mailed to a new mother. Since these samples have real costs, the manufacturer gives away only a tiny quantity – hoping to hook consumers and stimulate demand for many more<sup>66</sup>

O freemium nada mais é do que um modelo onde a plataforma oferece parte de seus serviços de forma gratuita, mas enquanto realizam o uso, são constantemente convencidos de que a versão paga possui mais recursos e traduz em maior valor agregado ao consumidor.

Há também, a utilização de publicidade. Nestes casos, o serviço é fornecido de forma gratuita, mas durante o uso, publicidades são utilizadas para atingir o consumidor durante o uso. Estes modelos são apenas alguns dos mais utilizados na atualidade.

É preciso ressaltar que existem realmente espécies de serviços totalmente gratuitos e sem finalidade lucrativa alguma, tendo como exemplo o Wikipedia, uma plataforma onde usuários podem complementar as informações de forma voluntária em prol de todos os demais que procurem por estes dados.

Neste sentido, Chris Anderson apresenta a ideia do gratuito real, mas presente em caráter de exceção:

In a sense, zero-cost distribution has turned sharing into an industry. In the monetary economy it all looks free – indeed, in the monetary economy it looks like unfair competition – but that says more about our shortsighted ways of measuring value than it does about the worth of what's created<sup>67</sup>

Embora este novo modelo de negócios aparente ser excelente para os usuários, eles também apresentam novos problemas, pois o uso dos serviços é regulamentado a partir de termos de uso, que possuem natureza jurídica de contratos de adesão, que devem ser aceitos ou a utilização não será liberada.

---

<sup>66</sup> ANDERSON, Chris. **Free! Why \$0,00 is The Future of Business**. Disponível em: <https://www.wired.com/2008/02/ff-free/>. Acesso em: 22 ago. 2019.

Não se trata do modelo de amostras grátis encontrado em todos os lugares desde prateleiras de perfumes a lojas de rua? Sim. Mas com uma significativa reviravolta. O modelo tradicional de amostras grátis consiste na distribuição de doces ou fraldas enviadas a uma mãe. Como tais amostras possuem um custo real, o fabricante apenas envia uma pequena quantidade – esperando que prenda e estimule os consumidores a buscarem por mais. (tradução livre)

<sup>67</sup> ANDERSON, loc. cit.

Em muitos casos, estes termos de uso podem trazer cláusulas anticonsumeristas, como:

Virtually all of these agreements contain some combination of anti-consumer clauses: forum selection, mandatory arbitration, bars on class action suits and the ability to make unilateral changes to the contract. Since online services are often based in one jurisdiction but accessible worldwide, if a business breaches their terms of service or commits some other civil wrong, consumers can be placed in an unfair position in a dispute or have no real opportunity for remedy<sup>68</sup>

Em se tratando dos termos de uso, é irreal solucionar estes problemas com o argumento de que se o usuário não concorda com os termos de uso, que simplesmente não utilize o serviço. Não é razoável, diante de um mercado onde a grande maioria dos negócios online utiliza das mesmas políticas, ainda que baseadas em uma jurisdição, seus serviços são acessíveis no mundo todo.

### 5.2.1 A monetização dos serviços e produtos online

Os serviços online gratuitos são uma espécie de negócio que monetiza o valor provido pelo usuário. De forma que o usuário não é obrigado a pagar para acessar o serviço, todavia, isto não significa que deverá ser totalmente gratuito, e sim que a utilização das principais funções da plataforma estará disponível independente de custo.

Trata-se, portanto, de uma estratégia para que o serviço cresça rapidamente, constitua uma base de usuários, a qual conduz ao ponto mais importante do serviço online gratuito: os usuários geram valor à plataforma.

A estrutura dessas plataformas costuma permitir que os usuários enviem algum tipo de conteúdo. A partir de então, o que, como e para quem, são as ferramentas trazidas e que farão seus usuários continuarem encaminhando informações. Quanto mais pessoas utilizam o serviço, maior a quantidade de conteúdo presente na plataforma e o valor da mesma cresce.

---

<sup>68</sup> SEBASTIAN, Kent. **No Such Thing as a Free Lunch**: Consumer Contracts and "Free" Services. Ottawa: Public Interest Advocacy Centre, 2014.

Praticamente todos estes acordos contêm uma combinação de cláusulas anticonsumo: seleção de fórum, arbitragem obrigatória, bares em ações coletivas e a capacidade de fazer alterações unilaterais do contrato. Desde serviços on-line são muitas vezes baseadas em uma jurisdição, mas acessível em todo o mundo, se uma empresa viola seus termos de serviço ou comete algum outro erro civil, os consumidores podem ser colocados em uma posição injusta em uma disputa ou não têm oportunidade real para solucionar.

Como já tratado, empresas em geral, visam o lucro, e sendo um serviço gratuito aos seus usuários, alguma forma de monetização deve ser gerada. Uma vez que não há pagamento direto pelo uso, o valor que os usuários geram à plataforma deve ser convertido em faturamento.

Embora seja um modelo de negócios destoante do tradicional, as plataformas online mais relevantes da atualidade seguem o modelo de serviços gratuitos, tais como o Instagram, Youtube, Gmail, Twitter, LinkedIn, Skype, Spotify, Dropbox, WhatsApp, Pinterest, e o mais utilizado no Brasil, o Facebook. Acerca desta rede social, Kent Sebastian explica:

The best example of this process is Facebook's rise to popularity. Facebook initially provided a structured way for people to display their pictures, find people with similar hobbies, and communicate with friends. The value of the platform was this ability to connect with others. As more and more people shared their information and connected with other users on Facebook, this data became increasingly valuable to advertisers. Facebook is now a publicly traded company with a market capitalization of around \$93 billion, with a substantial amount of their revenue generated through advertising<sup>4</sup>. The value users have provided to Facebook – namely, their personal information – has dwarfed the value Facebook initially provided to jump-start the platform<sup>69</sup>

Apesar de não requererem pagamento em moeda, não significa que eles não possuem custo algum. Os usuários estão dando algo de valor para estas plataformas, estando cientes ou não.

As informações mais básicas e comuns que usuários costumam fornecer são: nome completo, data de nascimento e suas preferências dentro da plataforma. Entretanto, ao invés de se ater somente a informações genéricas, os hábitos navegação do usuário podem ser rastreados sem seu expreso consentimento, mecanismo proporcionado pelas tecnologias disponíveis online.

---

<sup>69</sup> SEBASTIAN, Kent. **No Such Thing as a Free Lunch: Consumer Contracts and "Free" Services**. Ottawa: Public Interest Advocacy Centre, 2014. p. 8

O melhor exemplo deste processo é a ascensão do Facebook a popularidade. Facebook inicialmente forneceu uma forma estruturada para as pessoas a exibir suas fotos, encontrar pessoas com passatempos semelhantes, e se comunicar com amigos. O valor da plataforma foi esta capacidade de se conectar com os outros. À medida que mais e mais pessoas compartilharam suas informações e conectado com outros usuários no Facebook, esses dados se tornou cada vez mais valioso para os anunciantes. Facebook é agora uma empresa de capital aberto com uma capitalização de cerca de US \$ 93 bilhões do mercado, com uma quantidade substancial de sua receita gerada através advertising<sup>4</sup>. O valor que os usuários forneceram para Facebook - ou seja, suas informações pessoais - tem diminuído o valor Facebook inicialmente prevista para impulsionar a plataforma. (tradução livre)

O simples acesso do usuário que permite que determinado serviço acesse sua teia de contatos torna disponíveis informações que tem o potencial de aumentar o valor de negócio da empresa por serem dados que de outra forma, dificilmente poderia utilizá-los.

Um dos meios mais comuns de monetizar o valor que suas plataformas apresentam é a publicidade. Mas isso não significa que seja o único, pois existem diversas estratégias para fazê-lo, com os serviços “freemium”, que permitem o acesso gratuito de forma limitada, e também, de forma paga, uma versão completa de todas as funcionalidades.

Há ainda, licenciamento do conteúdo enviado pelo usuário, ferramentas onde o próprio usuário pode patrocinar sua postagem, os pedidos de doações e especialmente, a venda direta de dados dos usuários para outras empresas, como data brokers e agências de publicidade, são algumas das incontáveis estratégias de monetização possíveis.

Em um serviço gratuito ou inicialmente gratuito, o usuário pagante não constitui a base da plataforma. E mesmo que hajam muitos métodos para que o usuário venha a pagar, a grande maioria deles trabalha com a publicidade e demais formas de utilizar as informações dos usuários em benefício próprio.

Como todo negócio precisa gerar faturamento, aqui não é diferente. Vê-se então, que a plataforma irá proporcionar ao seu pagante, o serviço de forma que atenda aos seus interesses, visando aproveitar as vantagens de sua base de usuários. Em resumo, conforme Dmitri Fadeyev explica: “if the users aren’t going to pay for their product, the advertiser will pay for the users.”<sup>70</sup>

Para tratar desta situação, deve se lembrar que mesmo estabelecendo um baixo preço em um serviço cujo acesso já foi disponibilizado de forma gratuita, muito provavelmente a perda de usuários será relevante. Assim como um serviço criado baseado em pagamento desde o início, terá grandes problemas em constituir uma rede de usuários caso haja concorrentes que ofereçam algo similar sem custos.

Este comportamento de usuário foi comprovado com um estudo realizado pela University of Southern California School for Communication and

---

<sup>70</sup> FADEYEV, Dmitri. **Uncompromising Design** – Avoiding The Pitfalls of Free”. Disponível em: <http://www.smashingmagazine.com/2012/10/11/uncompromising-design-avoiding-pitfalls-free>. Acesso em: 22 ago. 2019.

Se os usuários não pagarem pelo seu serviço, o anunciante pagará por eles. (tradução livre)

Journalism <sup>71</sup>. Neste estudo foi constatado que metade dos usuários da internet nunca clicam em publicidade online, onde 70% disseram ser irritante. Todavia, neste montante, 55% disseram que preferem anúncios a pagar por conteúdo. À época do estudo, foi constatado que 49% dos usuários americanos faziam o uso de redes sociais como o Twitter, mas quando questionados se estariam dispostos a realizar pagamento para o uso, a porcentagem de aceitantes foi zero.

Portanto, embora as plataformas digitais sejam referências de gigantes dentro do mercado atual, devido ao método de monetização utilizado por elas, tornou-se inevitável o desequilíbrio entre os interesses da empresa e dos usuários, ocasionando descompasso, uma vez que os dados pessoais tornaram-se uma moeda valorizada dentro do mercado digital, ao passo que as empresas, por não exigirem pagamento de seus usuários, assim como toda empresa, precisa ter uma forma de faturamento. Nasce então, o conflito entre a utilização dos dados pessoais, sob ótica dos interesses dos usuários que os forneceram e das empresas que eventualmente os possuem.

### 5.3. A Publicidade Direcionada Online

É dentro da ciência mercadológica que os dados pessoais são convertidos em moeda de troca dentro da economia da informação. A organização dos dados de maneira a serem extraídos e convertidos em conhecimento útil tornou possível, conforme as palavras de Bruno Bioni, existir uma economia da vigilância, que tende a posicionar o cidadão como mero expectador de suas informações. <sup>72</sup>

Neste momento, torna-se indispensável demonstrar a maneira que os dados são utilizados em favor de uma parte enquanto o titular dos dados pessoais é deixado como sujeito passivo dessas informações.

Destarte, é preciso salientar o papel que o consumidor online possui dentro da economia atual. É dentro das redes que lhes são proporcionadas ferramentas que permitem a exposição de suas opiniões acerca dos mais diversos assuntos, mas especialmente, opiniões condizentes a experiências de consumo.

---

<sup>71</sup> PIERCE, Justin. **USC Annenberg Digital Future Study Finds Strong Negative Reaction to Paying for Online Services**. Disponível em: <https://annenberg.usc.edu/2010-usc-annenberg-digital-future-study-finds-strong-negative-reaction-paying-online-services>. Acesso em 22 ago. 2019.

<sup>72</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2018. p. 13



Dentro dessas plataformas, podem tanto criticar um produto, dizendo quais os pontos negativos deste, quanto elogiar outro, levantando seus aspectos benéficos.

E dentro deste sistema, independente de positivo ou negativa, a opinião dos consumidores é como um grande telão que é capaz de divulgar o produto, auxiliar em seu processo de produção, porque ficam então conhecidos seus aspectos para que sejam melhorados e produzidos em conformidade com as necessidades aparentes do mercado, de maneira nunca vista antes.

Foi deixada de lado a ideia de que o mercado apenas fornecia o que simplesmente desejava e o consumidor restrito a isso, pois o consumidor passa a ter papel fundamental, onde o mercado é capaz de modificar os direcionamentos acerca de um bem de consumo. E assim, o consumidor deixa de ser um mero passivo para ter participação ativa neste ciclo, exatamente por direcionar a produção e segmentar o mercado para que atinja o nicho ao qual o produto se destina.

É neste sentido que o marketing em geral passou por grandes mudanças, mas especialmente quando se trata da publicidade online de acordo com os modelos de negócio online.

Primeiramente, a publicidade é um elo de comunicação entre o consumidor e o fornecedor de um produto ou serviço, buscando, além de trazer informações sobre o bem, incentivar que ele venha a consumir efetivamente aquele produto, marca ou serviço, como se entende:

A teoria da linguagem vê a publicidade preliminarmente como uma construção discursiva decorrente da tensão entre interesses econômicos e valores simbólicos. Como a meta em publicidade é conseguir a adesão do público para assim garantir a venda de determinado produto, marca ou serviço, ela se vale de formas simbólicas que lhe possibilitem atingir esse objetivo <sup>73</sup>

A publicidade trabalha com o método da despersonalização das relações privadas, onde se trabalha com abordagens amplas, com o objetivo de atingir grandes quantidades de pessoas para propagar informações que versem a respeito de bens ou serviços afins de que essas se tornem consumidoras.

Os maiores exemplos da utilização deste método são os veículos mais difundidas de publicidade utilizadas até então, como os anúncios em revistas, televisão, rádio, outdoors. O anúncio é difundido de forma que atinja um grande

---

<sup>73</sup> PEREZ, Clotilde, BARBOSA, Ivan Santo. **Hiperpublicidade**: fundamentos e interfaces. v.1. São Paulo: Cengage Learning, 2017. E-book.

número de pessoas, independentemente de suas qualidades e preferências pessoais, atingindo aqueles que não apresentam possibilidade alguma de tornarem-se consumidores, como aqueles que são o efetivo público alvo do anunciante.

É neste aspecto que a publicidade tem verificado que não são meios com altos índices de eficiência, pois atingem um público sem a menor propensão ao consumo, gerando apenas custos com uma abordagem que não possui o retorno compatível com o dispêndio, e assim, tem substituído por outros tipos de abordagem, onde entra a ideia da publicidade direcionada.

A publicidade direcionada trabalha com o encaminhamento de informações a um público específico, que apresente maiores chances de consumir o bem ou serviço exatamente por suas características que demonstrem maior propensão ao consumo definindo um nicho que aumenta as chances de sucesso.

Utilizando dos meios despersonalizados, pode ser aplicada por exemplo, um anúncio sobre um produto de pele em uma revista voltada ao público feminino.

Aqui se encaixam os casos onde o sujeito pesquisa por determinados produtos, como por exemplo, tênis de corrida, demonstrando certo interesse em adquirir este produto, e a partir de então, o sistema passa a entender que este é um potencial consumidor, e passa a ofertar, por meio dos add-ons, o produto ao qual ele demonstrou maior interesse, seja pelo número de buscas por aquele bem em específico, ou até, ofertando a ele tênis similares ao que ele teve interesse.

O perfil do usuário é mapeado de forma que cada vez mais seja alcançado pela publicidade que potencialmente tem maiores chances de ser o público consumidor, e a cada clique, é gerada uma informação nova acerca daquilo que demonstra pertencer à sua zona de interesse.

É fundamental às empresas a utilização dessas informações, pois é através da conversão delas em conhecimento que transformam sua produtividade, aumentam seu lucro e constantemente se aprimoram através dos cliques de seus usuários. A publicidade mostra-se essencial aos negócios na atualidade, de forma que os clientes potenciais são atingidos e os antigos, de forma a serem constantemente lembrados da marca.

Em uma visão mais ampla acerca do uso dos dados, Larissa Kakizaki expõe:

o nosso comportamento não é analisado apenas pelas empresas, mas por todo mundo que tem acesso aos nossos dados. Isso apenas reforça a ideia mencionada anteriormente, na qual, além de crimes por meios eletrônicos que podem e são cometidos contra os usuários, há também a sua reputação nesse mundo digital. A dependência que criamos da internet deveria nos fazer pensar no quanto é importante resguardarmos nossa identidade; e, por esse motivo, os dados devem ser protegidos e as normas para isso precisam ser claras e transparentes<sup>74</sup>

É diante deste aspecto que a necessidade de proteção aos dados pessoais demonstra sua importância: eles não são meras informações geradas e desprezíveis, o mercado atual atribui grande valor a elas. E mais do que nunca, a identidade virtual é uma projeção da personalidade do indivíduo, onde qualquer ato praticado no mundo digital é plenamente capaz de gerar consequências de diversas maneiras.

---

<sup>74</sup> ALCANTARA, Larissa Kakizaki de. **Big Data e IoT: Desafios da Privacidade e da Proteção de Dados no Direito Digital**. 1. ed. São Paulo: Independente, 2017. *E-book*.

## 6 O CONSUMIDOR DE VIDRO

Com a evolução da tecnologia móvel, o monitoramento dos hábitos de navegação dos usuários tornou-se cada vez mais avançado, e a publicidade direcionada capacitada de maior precisão.

Uma das razões que proporcionou este desenvolvimento, se deve ao crescimento do mercado de aparelhos celulares, que cresceu exponencialmente, permitindo o acesso à internet a uma gama maior de usuários, incluindo a parcela da população que possivelmente não teria o acesso caso continuasse restrito aos modelos convencionais, como computadores, que demandam maiores custos.

É desta maneira que o celular é considerado o principal dispositivo de acesso à internet na atualidade, conforme pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação <sup>75</sup>, em 2017, 49% dos lares brasileiros dependiam de um celular para acessar a rede mundial de computadores.

A conexão é cada vez maior, não existindo mais hora nem lugar para que se tenha acesso à rede, ambientes on-line já se misturam com os off-line. A lógica mercadológica necessitou de mudanças para acompanhar a evolução da sociedade da informação, e uma delas foi que independente do local, seja um e-commerce ou estabelecimento físico, se não estiver presente na grande rede, corre o grande risco de inexistir offline também.

Isto se deve ao grande crescimento de ferramentas de busca na rede, onde empresários, de forma mais objetiva e direcionada, são capazes de divulgar seus serviços ou bens, da mesma forma que o consumidor usuário, ao ter acesso a essas informações, está mais propenso a buscar por esses bens ou serviços fornecidos por já ter tido um primeiro contato com eles de maneira on-line.

Um dos grandes mecanismos criados foi o monitoramento da localização geográfica (*global positioning system/ GPS*) dos smartphones, de forma que utiliza localizações de seus usuários para lhe enviar publicidade direcionada conforme a proximidade física.

---

<sup>75</sup> **Agência Brasil.** O Celular se Torna a Principal Forma de Acesso à Internet no Brasil. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-07/celular-se-torna-principal-forma-de-acesso-internet-no-brasil>. Acesso em: 06 ago. 2019.

Dados de localização são essenciais para diversos serviços fornecidos atualmente, tais como os restaurantes mais próximos ao local do usuário, e neste setor ainda, os serviços de entrega de comida por meio de aplicativos, que somente mostra os restaurantes mais próximos ao usuário.

O valor concebido aos dados de geolocalização é visível. Na compra do aplicativo de Waze, pela Google, pelo valor de 1,1 bilhão de dólares <sup>76</sup> em 2013. O serviço tem a funcionalidade de capturar a geolocalização de seus usuários, e baseado no conceito de rede social, em enviar e compartilhar informações, coleta dados de trânsito, e permite ao usuário marcar os locais em que ele esteve.

Utilizar destes dados é uma poderosa estratégia mercadológica, pois apresenta com maior precisão, anúncios com base na proximidade do usuário, não sendo por acaso que uma publicidade de um local próximo surja durante a navegação pelo smartphone.

## 6.1 O Controle do Consumidor por Meio de seus Dados Pessoais

Diante desta era de fácil acesso a informações, existe o caso da Pizza Hut, uma grande franquia norte-americana especializada em pizzas e massas, a qual adotou um sistema de análise de preferências de seus clientes com o objetivo de tornar suas estratégias de negócio mais produtivas.

Com este sistema de análise preditiva, a franquia seria capaz de sugerir sabores de pizzas baseando-se nos desejos subconscientes de seus clientes <sup>77</sup>. A questão então passaria a ser que dados eles utilizariam para fazer predileção das preferências dos consumidores, conforme a análise de possibilidades a seguir:

Talvez a empresa pudesse analisar preferências de seus consumidores através dos seus "Likes" no Facebook ou, ainda, afiliar-se às companhias de seguro de saúde que têm a capacidade de prever quando uma pessoa ficará doente, visando sugerir opções mais saudáveis e, assim, fomentar sua estratégia de marketing. Poderia até mesmo recusar a venda a clientes com problemas de crédito ou sugerir meios alternativos de pagamento com base na sua atual situação financeira e na classe social a que pertencem seus potenciais clientes. Produtos diferentes poderiam ser ofertados para

---

<sup>76</sup> **Site CanalTech.** Agora é Oficial: Google compra Waze por US\$ 1,1 bilhão. Disponível em: <https://canaltech.com.br/mercado/Agora-e-oficial-Google-compra-Waze-por-US-11-bilhao/>. Acesso em: 8 ago. 2019.

<sup>77</sup> MONTEIRO, Renato Leite. BIONI, Bruno. Que tal uma pizza de tofu com rabanetes? Você vai adorar!. **Huffpost.** Disponível em: [https://www.huffpostbrasil.com/renato-leite-monteiro/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar\\_a\\_21682549/](https://www.huffpostbrasil.com/renato-leite-monteiro/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar_a_21682549/). Acesso em 08 de ago. 2019.

regiões mais precárias das cidades. Estas esparsas informações, por mais que sejam oferecidas por fontes diversas, poderiam todas serem agregadas por meio do Registro Civil Único, quando este fosse implementado pelo Governo Federal, conforme recentemente sugerido através de projeto de lei elaborado pelo Tribunal Superior Eleitoral<sup>78</sup>

A partir dos inúmeros dados que a empresa teria em prol de sua estratégia de marketing, surgem inúmeras consequências possíveis decorrentes de seu uso, que só depende da vontade do consumidor, que se torna mero fantoche, onde inclusive a pizza que ele venha a consumir não decorreu intrinsecamente uma escolha própria.

No ano de 2004, um texto que simulava um pedido de pizza pelo telefone em 2010, circulou e chegou a ser reproduzido em uma prova de processo seletivo do Instituto de Tecnologia e Aeronáutica. Com a leitura, é possível visualizar a ironia da visão de tratamento de dados pessoais que havia para um futuro, e comparar com o caso que realmente ocorreu, com o Pizza Hut.<sup>79</sup>

A narração descrevia um caso onde o atendente do delivery tinha acesso a uma espécie de banco de dados que aglutinava informações do cliente de diversas naturezas, como histórico de saúde, preferências, situação financeira, como um número de identificação nacional.

A partir deste identificador, o atendente já passou a ter acesso ao endereço residencial, comercial, assim como os números de telefone que o cliente possuía, consulta a ficha médica do sujeito e sugere que ele mude seu pedido para um mais saudável, porque o seu seguro de vida proíbe que ele faça escolhas de risco à sua saúde.

Assim, termina escolhendo conforme sugestão do atendente uma pizza de tofu e rabanetes pois contava em seu banco de dados que em determinada data e hora, o sujeito havia consultado um site de receitas relacionadas e o tempo que permaneceu conectado. No momento do pagamento, seu cartão de crédito é recusado pois o atendente alega que o limite foi ultrapassado, o cliente escolhe pagar em dinheiro, e o telefonista recusa novamente pois diz que ele não tem saldo em conta, e possui dívidas em seu nome.

---

<sup>78</sup> MONTEIRO, BIONI, loc. cit.

<sup>79</sup> Encomendando uma pizza em 2010. **Site Devmedia**. Rio de Janeiro. Disponível em: <https://www.devmedia.com.br/forum/encomendando-uma-pizza-em-2010/125441>. Acesso em 09 de ago. 2019.

Conforme percebia a avalanche de informações que o atendente possuía sobre sua pessoa, o sujeito acaba insultando o funcionário, que acaba dizendo para que ele não o faça pois ele já tem uma condenação criminal em seu nome, citando prontamente o crime e a data do feito.

Ao fim, o cliente se sente tão sobrecarregado que ameaça se atirar da janela, e o atendente ironicamente apenas diz que ele irá machucar os joelhos por morar no andar térreo.<sup>80</sup>

Apesar da narração ter sido escrita em 2004, simulando o futuro que trata de maneira tão invasiva as informações pessoais de seus cidadãos, inclusive banalizando-os, pois através de um único número de registro, um simples atendente de delivery passa a ter acesso absolutamente todos os dados pessoais do cliente que simplesmente gostaria de realizar um pedido de pizza.

Ao analisar o caminho que o tratamento de dados pessoais vem tomando, coincidentemente uma franquia de pizzas já possui o poder de acesso a informações de seus clientes para os fins que desejar, verifica-se a clara banalização dos dados pessoais.

É claro que um delivery não precisa ter acesso ao histórico criminal do cliente, ao seu saldo bancário, são informações muito relevantes para o usuário, mas certamente, não essencial para o desempenho de sua prestação de serviço, que deveria ater-se ao endereço, telefone e meio de pagamento a ser empregado na venda.

A partir de então, inúmeros casos da atualidade vêm realmente demonstrando este livre poder sobre os dados pessoais, cada uso sendo capaz de atender aos interesses de quem o aplica, como o caso da varejista americana Target.

## 6.2 O Caso Target

A gigante Target, uma grande varejista estadunidense, teve um caso que ganhou grande repercussão por utilizar do Big Data como ferramenta de estudo de comportamento de seus consumidores, baseando-se no histórico de navegação e

---

<sup>80</sup> Encomendando Uma Pizza Em 2010. **Site Devmedia**. Rio de Janeiro. Disponível em: <https://www.devmedia.com.br/forum/encomendando-uma-pizza-em-2010/125441>. Acesso em 09 de ago. 2019.

informações captadas pela própria loja, criando um perfil específico para cada cliente, levando a descobrir a gravidez de uma adolescente antes de seu pai.

Primeiramente, a varejista realizou uma campanha onde suas clientes informavam quando estavam grávidas e a data estimada do nascimento do bebê. Com estas informações em mãos, a Target passou a analisar os hábitos de compras destas clientes, notando que elas passavam a comprar produtos específicos, como vitaminas e produtos com fragrância suave ou sem cheiro.

A partir de então, foi analisado que o padrão costumava se repetir, sendo possível saber quando havia uma cliente grávida mesmo quando ela não informava à empresa. E assim, a empresa direcionava a essas clientes, campanhas direcionadas em produtos que estivessem relacionados a gravidez.

Um desses direcionamentos foi enviado ao pai de uma cliente, que se revoltou com os cupons, uma vez que entendeu estarem influenciando sua filha a engravidar. Ocorreu que ele buscou a empresa para reclamar acerca disso, todavia, após o evento, descobriu que sua filha já estava grávida.

Esta foi uma das polêmicas pioneiras, onde a análise de dados aplicada em função dos objetivos da empresa foi capaz de descobrir um fato antes mesmo das pessoas próximas do perfil analisado.

### **6.3 O Caso 23andme**

Apesar de tudo, o histórico de pesquisas, por exemplo, ainda não é considerado algo que possa causar grandes consequências na vida de uma pessoa. Aqui temos um caso onde dados pessoais personalíssimos entram em jogo, os quais referem-se a informações genéticas.

A empresa 23andMe, desenvolvida com investimentos da Google, uma proximidade que possui devido a sua CEO, Anne Wojcick, ser casada com Sergey Brin, cofundador e ex-presidente da Google, quando fundada.

Este empreendimento buscava proporcionar o acesso a análises genéticas para um público maior e de forma mais acessível, de modo que o consumidor pode adquirir seu kit para testes em mercados e farmácias. A partir de então, segue as instruções do material, coleta amostras de saliva e as envia pelo correio para a empresa realizar as análises necessárias.



O cliente pode escolher quais os testes e análises que deseja realizar, conforme o kit que adquiriu, estando disponíveis serviços como investigação de ancestralidade para formação de árvore genealógica, análise do DNA da família, encontrar parentes na plataforma da empresa e que já estejam cadastrados no banco de dados, além de toda uma análise de doenças as quais o material indique que a pessoa tem predisposição a desenvolver, como diabetes tipo 2, Alzheimer, incluindo análises que mostram que a pessoa carrega genes de algumas doenças, portanto, mostra que ele é mais suscetível a desenvolvê-las, como fibrose cística e anemia falciforme.<sup>81</sup>

Isto tudo por um preço bem inferior ao que costumava ser cobrado para realizar análises de DNA, que variava em torno de mil dólares, contra os preços da empresa, que variam de noventa e nove dólares a cento e noventa e nove dólares pelo serviço completo, que está disponível em cinquenta países.

Todavia, no ano de 2018, a empresa anunciou uma parceria com a gigante farmacêutica GlaxSmithKline (GSK), uma das mais poderosas do mundo, faturando em torno de quarenta bilhões de dólares por ano. Nesta negociação, a GSK se comprometeu a investir 300 milhões de dólares na 23andMe<sup>82</sup>, e em troca, teria o acesso ao banco de dados de seus clientes.

E esta foi uma notícia chocante para todos que tinham utilizado dos serviços da empresa, uma vez que a grande maioria não estava ciente da possibilidade de compartilhamento de seus dados com outras empresas, ainda que a possibilidade estivesse presente nos termos de uso.

A utilização de informações genéticas é um tema sensível, conforme expõe a matéria:

O DNA de uma pessoa pode ser usado contra ela: os planos de saúde poderiam cobrar mais caro de quem é predisposto a certas doenças ou comportamentos, e esse mesmo critério poderia ser adotado por empresas para vetar a contratação de alguém. Num cenário mais radical, dados genéticos também poderiam ser explorados por governos xenófobos ou de inclinação eugênica<sup>83</sup>

---

<sup>81</sup> 23andMe. Disponível em: <https://www.23andme.com/?myg=true>. Acesso em: 18 jul. 2019

<sup>82</sup> MARTINEAU, Paris. How to sign away the rights to your DNA. **Site The Outline**. Disponível em: <https://theoutline.com/post/5555/how-to-sign-away-the-rights-to-your-dna?zd=2&zi=rewxmeqw>. Acesso em 19 de jul. 2019,

<sup>83</sup> GARATTONI, Bruno. 23andMe vai entregar DNA dos seus usuários para gigante farmacêutica. **Site Super Abril**. Disponível em: <https://super.abril.com.br/comportamento/23andme-vai-entregar-dna-dos-usuarios-para-gigante-farmacautica/>. Acesso em: 20 de jul. 2019.

São informações de cunho personalíssimo, cuja natureza pode ser desviada para diversas funcionalidades que a pessoa que as forneceu não tem controle sobre. Significa, portanto, que muito além do fim que ele esperava destes dados, existem muitos outros, e que podem gerar consequências positivas e negativas para ele, pessoas relacionadas a ele, e até futuramente, aos seus descendentes.

#### **6.4 O Caso Cambridge Analytica**

Um dos casos mais polêmicos da atualidade envolvem a utilização de dados pessoais provenientes de redes sociais, e neste caso específico, a empresa privada Cambridge Analytica e suas estratégias de análise e mineração de dados em processos eleitorais.

A Cambridge Analytica consiste em uma empresa de assessoria política a qual realizou o uso de análise de dados para favorecer as campanhas políticas daqueles que a contratavam, assim como difundir ideias, posicionamentos, visando popularizar seus objetivos.

Uma das maiores polêmicas envolvendo esta empresa dizem respeito às eleições presidenciais americanas de 2016, uma vez que ela trabalhou na campanha que resultou na eleição de Donald Trump como presidente dos Estados Unidos, onde seu trabalho envolveu análise de dados dos eleitores americanos, aos quais teve como principal fonte o Facebook e direcionamento de todo o tipo de mensagens, publicações, artigos, vídeos em prol do candidato, conforme o perfil de cada eleitor.

Sendo assim, a empresa utilizou de dados do Facebook, os quais eram fornecidos por usuários que simplesmente aceitavam termos de uso de aplicativos e diversos serviços conectados com a rede sem realizar a devida leitura, e com este aceite, passavam a prover acesso aos dados de todos os usuários que se encontravam em sua rede de amigos, crescendo exponencialmente o número de dados pessoais a que a Cambridge Analytica tinha acesso.

É necessário frisar que cada usuário tem pegadas na internet, conforme o documentário *The Great Hack* demonstra, a cada passo, a cada clique, cada pesquisa, like, compra, é absorvido e condensado levando a um perfil onde as ações de cada um torna-se previsível, sendo assim possível que a inteligência

artificial seja capaz de direcionar individualmente, aquilo que melhor se encaixa diante de cada perfil.

Mas, diferente do que é comumente divulgado, os dados pessoais não são apenas utilizados para uma melhor performance de anúncios publicitários nas redes sociais, as gerações que já tem o contato com a internet há tempos, já não se incomodam com os “ads” em todas as plataformas que utilizam, é natural.

O grande poder dos dados pessoais é a capacidade de estudo comportamental sendo utilizado como mecanismo de convencimento eficiente ao ponto de mudar opiniões e ideias que as pessoas tenham acerca de determinado assunto. Desta forma, o direcionamento de informações a depender de quem o controla, é estrategicamente posicionado para que o usuário seja convencido daquilo que esteja à vontade de quem possui o poder.

É a ideia de realizar mudanças, e para que elas aconteçam, é introduzido e direcionado somente aquilo que é do interesse de quem possui controle sobre os dados e sabe fazer o uso deles ao seu favor, seja com o objetivo de mudar um posicionamento que o usuário tenha, ou trabalhar em direção do usuário indeciso para que ele se veja inclinado à posição desejada por quem possui o controle sobre seus dados pessoais.

Brittany Kaiser, ex- funcionária da Cambridge Analytica, que trabalhou como diretora de desenvolvimento comercial da empresa no período de 2015 a 2018, e uma das pessoas que denunciaram a corporação , expôs que os dados pessoais são como um bumerangue, você envia seus dados, eles são analisados e voltam para você como mensagem direcionada para mudar seu comportamento.

Diante deste cenário de falta de controle sobre os próprios dados pessoais, a inquietação e indignação fez com que o professor americano David Carroll peticionasse para que a companhia, de forma transparente, liberasse os dados que possuía acerca dele, conforme a investigação do The Guardian:

An American professor who is using UK law to try to reclaim data that may be held by Cambridge Analytica has told The Guardian he is encouraged that regulatory pressures on both sides of the Atlantic could force companies to be more transparent about their handling of personal information.

[...] David Carroll, an associate professor at Parsons School of Design in New York, filed a statement in the high court in London in support of a claim

to recover his data and reveal its source, citing Cambridge Analytica and SCL Elections Ltd, described as its parent company.<sup>84</sup>

O ato do professor gerou muitas expectativas perante o que a empresa viria a fazer, por ter sido ato inédito um cidadão realizar este tipo de requisição. Em janeiro de 2019, teve fim o prazo dado pela suprema corte inglesa para que os dados extraídos em nome de David Carroll, e conforme reportagem da revista Exame, a empresa foi condenada a pagar uma multa de 15.000 libras (19.100 dólares, 16.700 euros), além de ter de pagar os custos judiciais no valor de 6.000 libras.<sup>85</sup>

Isto porque a Cambridge Analytica recusou-se a fornecer os dados e se declarou culpada, descumprindo a ordem judicial. Diante do ocorrido, o advogado representante do Comissário de Informação Britânico (ICO), apresentou a quantidade de dados que a companhia foi capaz de extrair a partir dos usuários do Facebook, que equivalem a 81 bilhões de páginas impressas, como exposto a seguir:

O advogado representante do Escritório do Comissário de Informação britânico (ICO) afirmou perante o tribunal que a Cambridge Analytica conseguiu reunir o equivalente a 81 bilhões de páginas impressas de dados sobre os usuários do Facebook.

[...] Segundo o advogado da ICO, a empresa tinha dito a Carroll: “Você não tem direito de fazer (uma solicitação de acesso a dados), como um membro dos talibãs sentado em uma caverna no canto mais remoto do Afeganistão também não tem direito de fazer isso”.

Mais tarde, um dos executivos da Cambridge Analytica disse à ICO que “esperava não continuar sendo assediado com este tipo de pedidos”.

Admitindo sua culpa por descumprir a ordem, a empresa ressaltou, no entanto, que “este julgamento não está relacionado nem sugere o uso indevido de dados nem nenhuma ação potencial relacionada com isso”.<sup>86</sup>

<sup>84</sup> **The Guardian**. Disponível em: <https://www.theguardian.com/uk-news/2018/mar/20/david-carroll-cambridge-analytica-uk-courts-us-professor>. Acesso em: 03 ago. 2019.

Um professor americano que está usando a lei britânica não tentar recuperar dados que podem ser detidos por Cambridge Analytica disse ao The Guardian que ele é encorajado que as pressões regulamentares em ambos os lados do Atlântico poderiam forçar as empresas a serem mais transparentes sobre a sua manipulação da informação pessoal.

[...] David Carroll, um professor adjunto na Parsons School of Design, em Nova York, apresentou uma declaração na Alta Corte de Londres em apoio de um pedido para recuperar seus dados e revelar sua fonte, citando Cambridge Analytica e SCL Eleições Ltd, descrita como sua controladora. (tradução livre)

<sup>85</sup> Cambridge Analytica se declara culpada por uso de dados do Facebook. **Site Exame**. Disponível em: <https://exame.abril.com.br/tecnologia/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook/>. Acesso em 05 ago. 2019.

<sup>86</sup> Cambridge Analytica se declara culpada por uso de dados do Facebook. **Site Exame**. Disponível em: <https://exame.abril.com.br/tecnologia/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook/>. Acesso em: 05 ago. 2019.

Neste ponto, é visível que a empresa não esperava tamanha repercussão diante do processo judicial, pois o pedido não apresentava precedentes, e ainda, houve inquietação por parte daqueles que acompanharam o seu andamento, que visualizaram a impotência do usuário comum dentro do ambiente digital. A empresa cessou suas atividades após este escândalo.

Muito além dos usos atribuídos aos dados pessoais dos usuários do Facebook, de responsabilidade atribuída à Cambridge Analytica, houve também a responsabilidade da rede social, que teve papel essencial como fonte de grande parte dos dados utilizados, especialmente quando passou a se discutir a venda de dados pessoais dos usuários pelo Facebook.

Para isto, Mark Zuckemberg, cofundador da rede social, foi intimado a depor, para esclarecer como a empresa conseguiu o acesso aos dados de 50 milhões de usuários da rede, e esta foi a declaração dele, conforme investigação do CNN:

In his testimony, Zuckerberg told lawmakers that "we don't sell data to anyone." He also said, "This is the most important principle for Facebook: Every piece of content that you share on Facebook, you own and you have complete control over who sees it, and how you share it, and you can remove it at any time."

But now, it appears that these weren't accurate statements. According to the Times, Facebook allowed more than 150 companies to view private user data, including their private messages. Companies granted access include not only giants such as Microsoft, Amazon and Spotify but also the Chinese company Huawei and Russian company Yandex, potentially raising national security concerns on top of privacy ones<sup>87</sup>

Após a repercussão tida no caso, a imagem de Mark, e especialmente a visão tida pela sociedade diante do Facebook, deixou de ser apenas uma empresa

---

<sup>87</sup> ALAIMO, KARA. Mark Zuckerberg has lost all credibility with Congress - and the rest of us. **CNN, Estados Unidos**. Disponível em: <https://edition.cnn.com/2018/12/21/opinions/mark-zuckerberg-misled-congress-privacy-nyt-alaimo/index.html>. Acesso em 05 de ago. 2019

Em seu depoimento, Zuckerberg disse aos legisladores que "nós não vendemos dados a ninguém." Ele também disse: "Este é o princípio mais importante para o Facebook: Cada pedaço de conteúdo que você compartilhar no Facebook, você possui e você tem controle completo sobre quem o vê, e como você compartilhá-lo, e você pode removê-lo a qualquer momento".

Mas agora, parece que estes não eram declarações precisas. Segundo o Times, o Facebook permitiu que mais de 150 empresas para ver os dados do usuário privadas, incluindo as suas mensagens privadas. Empresas concedido acesso incluem não apenas gigantes como Microsoft, Amazon e Spotify, mas também a empresa chinesa Huawei e empresa russa Yandex, potencialmente levantando preocupações de segurança nacional em cima de uns privacidade. (tradução livre)

que todos faziam o uso indiscriminado para visualizar então a capacidade e o poder que eles possuem.

Apesar de afirmar que sua empresa não vende os dados de seus usuários para ninguém, como apresentado na investigação, o Facebook permitiu mais de 150 empresas terem o acesso aos dados pessoais de seus usuários, incluindo mensagens privadas, estando entre elas gigantes americanas como Microsoft, mas também companhias chinesas e russas, o que abala a segurança nacional americana.

Em se perguntando quais são as formas utilizadas para que o usuário conceda seus dados pessoais de forma consentida, mas não necessariamente consciente, trata-se da vinculação do perfil do Facebook a algum serviço ou programa para não haver a necessidade de criar um login único todas as vezes, sendo extremamente cômodo, visando o rápido acesso.

Todavia, estes serviços e programas sempre apresentam termos de uso, cujo usuário deve preencher a opção de aceita-los para que o uso seja liberado, e neste termo a concessão de acesso aos dados do usuário costuma estar presente, inclusive, nos serviços utilizados pela Cambridge Analytica, a concessão de acesso aos dados dos amigos da rede social.

## 6.5 O Caso FaceApp

Ainda relacionado a serviços difundidos pelas redes sociais, no ano de 2019, um destes serviços gerou preocupações. Um aplicativo chamado FaceApp capturava a imagem do usuário e a editava, transformando em foto o rosto da pessoa como estivesse envelhecida. O grande número de usuários que fez o uso do aplicativo levou a investigações acerca do serviço, e este foi o resultado:

According to FaceApp's terms of service, when you use the app you grant it a "perpetual, irrevocable, nonexclusive, royalty-free, worldwide" license to do whatever it wants with your photos. However, while this may be awful, it's worth pointing out that it's the same as the privacy policy of basically every other tech service and platform. <sup>88</sup>

---

<sup>88</sup> MAHDAWI, Arwa. **Is FaceApp an evil plot by 'the Russians' to steal your data?** Not quite. Disponível em: <https://www.theguardian.com/commentisfree/2019/jul/18/faceapp-privacy-data-russians>. Acesso em: 13 ago. 2019.

De acordo com os termos de uso do FaceApp, quando você utiliza o aplicativo, fornece a eles uma "perpétua, irrevogável, não exclusiva, isenta de royalties, mundial" licença para fazer o que desejarem

Esta preocupação que surgiu entre os internautas certamente é fruto da incerteza e desconfiança plantadas no mundo digital após o caso de venda de dados pelo Facebook. Todavia, mesmo aqueles que não participaram do *#faceappchallenge*<sup>89</sup> por estarem preocupados com sua privacidade, não podem ficar tranquilos ainda.

Em artigo publicado por alunos da Universidade de Cornell, as maiores quantidades de dados concentram-se sob posse de grandes corporações como Google e Facebook, que respectivamente, utilizou 200 milhões de imagens para reconhecimento facial de 8 milhões de identidades, e 500 milhões de imagens para reconhecimento facial de 10 milhões de identidades.<sup>90</sup>

Assim, embora não tenha diretamente se exposto aos termos e fornecido o livre consentimento para utilização de sua imagem, ela muito provavelmente já se encontra em bancos de dados com o objetivo de treinar alguma inteligência artificial.

Entretanto, a situação atual torna-se ainda mais complexa quando não é mais necessário que a foto seja postada para treinar uma tecnologia de inteligência artificial. Em maio de 2019, foi denunciado que a Universidade de Colorado, localizada em Colorado Springs, esteve fotografando secretamente seus estudantes para um estudo sobre reconhecimento facial, conforme o jornal *Colorado Springs Independent* publicou.<sup>91</sup>

Imagens de mais de 1700 pessoas foram coletadas entre os anos de 2012-2013 sem o seu conhecimento ou consentimento, destinadas ao banco de dados para treinamento de algoritmos de reconhecimento facial. É necessário destacar que os recursos e incentivos para este projeto foram proporcionados pela Inteligência dos Estados Unidos e agências militares.

---

com suas fotos. Todavia, embora isto seja terrível, é válido apontar que é a mesma política de privacidade de basicamente qualquer outro serviço ou plataforma online. (tradução livre)

<sup>89</sup> Desafio FaceApp (tradução livre)

<sup>90</sup> BANSAL, Ankan, et al. **UMD Faces**: An Annotated Face Dataset for Training Deep Networks. Disponível em: <https://arxiv.org/abs/1611.01484>. Acesso em 17 ago. 2019.

<sup>91</sup> STANLEY, J. Adrian. **UCCS secretly photographed students to advance facial recognition technology**. Disponível em: <https://www.csindy.com/coloradosprings/uccs-secretly-photographed-students-to-advance-facial-recognition-technology/Content?oid=19664437>. Acesso em 15 ago. 2019.

## 6.7 A Problemática dos Dados Pessoais e sua Extensa Gama de Alcance

Desta forma, é possível auferir o poder que a internet e todos os mecanismos que a acompanham, podem ser utilizados de inúmeras maneiras para atender os interesses daqueles que detêm o poder sobre determinados dados.

Os dados, por si só, não representam nada. O poder que o dado pessoal possui somente se manifesta quando é organizado visando um determinado fim. O caso Target demonstra isto da forma mais simples: ao invés de somente armazenar informações do histórico de compras de seus clientes, eles foram organizados de maneira a melhorar suas estratégias de venda e marketing.

Ao analisar o sistema do Pizza Hut em comparação ao texto “Comprando uma pizza em 2010”, é possível identificar o incômodo causado pelo excesso de informações pessoais detidos por terceiros, a ponto de escolherem o sabor da pizza que você irá consumir em prol de sua saúde e questionarem como você vai realizar o pagamento por identificar que o seu limite de crédito já foi ultrapassado.

A venda de dados genéticos sem a ciência de seus proprietários demonstra uma reviravolta na visão que prevalecia sobre os dados pessoais e que vinham sendo tratados de forma negligente por seus efeitos aparentemente estarem restritos ao meio digital.

Os dados pessoais constituem um instrumento, cuja presença ou ausência proporciona a possibilidade ou impossibilidade de praticar diversas ações. A venda de dados que permite identificar o sujeito será capaz de gerar alguma restrição futura, da qual nem mesmo ele possuía ciência, como não conseguir realizar a contratação de um plano de saúde mais barato pela empresa ter um histórico de sua árvore genealógica que consta a possibilidade de desenvolvimento de determinada doença genética. Isto tudo porque foi contratado um serviço que intencionava ser apenas um exame de DNA.

Além disso, a utilização dos dados pessoais permite, inclusive, uma manipulação de seus usuários, como no caso da empresa Cambridge Analytica, que utilizou dados de usuários do Facebook para enviar publicações contendo informações direcionadas aos perfis que consideravam alvo.

Por meio de análise dos dados dos usuários do Facebook, especialmente americanos e ingleses, a empresa foi capaz de bombardear a rede



com publicações, eventos, vídeos que fossem capazes de fazer as pessoas verem o mundo de forma congruente aos interesses dos candidatos que os contrataram.

Ao final, a estratégia mostrou-se muito eficiente, todavia, os meios utilizados por eles para conseguir estes dados não foram expostos, pois a ação judicial protocolada pelo professor David Carroll com o pedido de que a empresa liberasse os dados que possuía sobre ele não foi cumprida. A Cambridge Analytica se autodeclarou culpada e realizou pagamento de multa. Mas a lide continua não resolvida, pois ainda não existe o controle dos usuários acerca dos dados que existam em seu nome espalhados pela internet.

As problemáticas envolvendo o uso de dados pessoais continuará existindo, sendo em maior ou menor proporção, como ocorreu no ano de 2019, com o serviço “FaceApp”, que apresentou mobilização de usuários preocupados com o que leram nos termos de uso do serviço, como a permissão de utilização perpétua do serviço pelas fotos do usuário.

Atualmente, existem inúmeras tecnologias com a finalidade de estruturar um banco de dados de emoções. Estes dados seriam captados através de mecanismos capazes de interpretar as emoções dos usuários de forma a direcionar conteúdos compatíveis com o que o usuário demonstra estar sentindo.

Neste sentido, as gigantes do mercado como Microsoft, Google e Apple, vem estudando o sistema de processamento de movimentos, através de um chip sensor, denominado M7, que seria capaz de identificar o deslocamento dos usuários para precisar como ele estaria mentalmente quando utiliza algum serviço. Há ainda, estudos para estabelecer um sistema detector de expressões faciais para os usuários do Youtube, permitindo a avaliação do usuário, em relação aos vídeos que apresenta reações melhores, e também aos criadores de conteúdo da plataforma, que possivelmente teriam que apresentar reações melhores dos usuários para ter um maior alcance na rede.

Desta forma, o usuário mostra-se cada vez mais à mercê da vontade das empresas que possuem em seu poder, os dados pessoais dos usuários, sendo que independem de serem seus usuários ou de terceiros, pois, devido à sua valorização no mercado digital, ocorrem suas cessões ou vendas.

A sociedade da informação traduz novos desafios para a pessoa humana, especialmente diante da monetização de seus dados pessoais, que conforme Danilo Doneda expõe: algumas normativas específicas para a proteção da

pessoa surgem então em torno de necessidades específicas – seja no caso da problemática pesquisa genética ou, no nosso caso, em torno da proteção dos dados pessoais.<sup>92</sup>

Trata-se de um novo direito da personalidade, um prolongamento da pessoa, que interfere em áreas que excedem o âmbito em que foram inseridas, que justifica a necessidade de uma tutela jurídica específica, tratando de pontos como o direito de cesso e a retificação de dados, por exemplo.

A afirmação apresentada por Bruno Bioni, reflete o parâmetro atual de valoração dos dados pessoais na sociedade da informação, dizendo que: os dados pessoais são o petróleo, insumo ou uma commodity, estando para a economia da informação como a destruição do meio ambiente estava para a economia industrial.

<sup>93</sup>

É neste sentido que o fim da privacidade se mostra latente no sistema econômico atual, onde os dados pessoais são a moeda que sustenta, movimenta e valoriza os novos modelos de negócios, assim como políticas públicas.

Conforme diretrizes emitidas pela Organização para o Desenvolvimento e Cooperação Econômica na década de 1980, e atualizadas recentemente, as leis de proteção de dados visam conferir segurança jurídica ao cidadão, e paralelamente, estabelecer aos agentes que farão uso destes dados, seja público ou privado, diretrizes para a utilização dos mesmos. O objetivo preponderante sendo conferir confiança entre as partes de modo que o ecossistema continue em constante crescimento.

A proteção de dados, portanto, apresenta dupla função, de fazer com que os dados sejam passíveis de tratamento competitivo no mercado, e ao mesmo tempo, que o usuário se sinta seguro no ambiente digital.

A LGPD caracteriza um marco da regulamentação jurídica acerca destas previsões no Brasil, pois estabeleceu regramentos em lei a situações que somente leis esparsas previam, que por vezes, conflitavam entre si.

A referida lei apresenta como objetivos proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, além de elencar em seus fundamentos preceitos

---

<sup>92</sup> DONEDA, Danilo. **Da Privacidade à proteção dos dados pessoais**. Rio de Janeiro: renovar, 2006, p. 100 .

<sup>93</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2018, p. 107.

relevantes como o respeito à privacidade e o desenvolvimento econômico e tecnológico e a inovação<sup>94</sup>.

O objetivo da lei é conciliar estes elementos de forma que o usuário não seja violado em seus direitos fundamentais, tais como privacidade, honra, imagem, sua autodeterminação informativa, ao tempo que a exploração destes dados cumpra sua finalidade, respeitando a livre iniciativa, o desenvolvimento econômico e tecnológico e a inovação.

Desta forma, visualiza-se a relevância de permitir ao cidadão que tenha controle sobre os próprios dados pessoais como a principal medida para assegurar que a sociedade da informação mantenha seu fluxo informacional de forma a atingir suas finalidades e não prejudicando o livre desenvolvimento da pessoa natural. Não se trata apenas de conseguir o consentimento do usuário para utilização de seus dados, uma vez que grande parte das empresas trabalha com métodos que conseguem o consentimento, mas não de forma consciente do cidadão, como visto com os termos de uso.

Portanto, resta estudar quais são as estratégias que poderão ser utilizadas de forma a concretizar a dupla finalidade da LGPD, facilitação de trocas informacionais e a proteção aos direitos fundamentais dos usuários. Uma vez que o fluxo informacional apresenta relevância essencial na sociedade da informação, e ao mesmo tempo, devendo transparência no uso dos dados aos cidadãos.

---

<sup>94</sup> Art. 1º e 2º da lei

## 7 OS MEIOS DE TUTELA DOS DADOS PESSOAIS

A partir da análise da forma operacional do consentimento dentro do mercado de dados pessoais, é visualizável que ele é fornecido da forma encontrada pelos agentes atuantes na economia da informação: através de políticas de privacidade e termos de uso.

Desta maneira, colhe-se o consentimento necessário para legitimar qualquer utilização que venha a ser realizada acerca dos dados pessoais.

A natureza das políticas de privacidade apresenta-se essencialmente como contratos de adesão, que destacam a assimetria do mercado, uma vez que não informa e não qualifica o usuário para que tenha o efetivo controle sobre suas informações pessoais.

As tecnologias da informação se mostram dirigidas pela massificação das relações de consumo, onde o papel do usuário acaba sendo apenas concordar ou discordar dos termos expostos, em um tudo ou nada, trazendo à tona a ideia de que, caso não concorde com as condições impostas, simplesmente não utilize o serviço, algo que não se mostra razoável na sociedade da informação.

Desta forma, ao concordar com os termos, o usuário perde o total controle sobre seus dados, uma vez que após a concordância, o fornecedor não é transparente acerca dos usos que a informação terá, passando a ter, após a concordância, o controle do fluxo informacional do usuário, que não possui qualquer mecanismo de rastreamento do uso de seus dados.

Os usuários não têm o poder de negociação em prol de suas preferências, e com esta forma de contratação, o usuário apresenta papel passivo no controle de seus dados, e pela inefetividade da informação concedida pelos termos de uso, grande maioria não possui a consciência da importância de controle de suas informações pessoais. Acerca da inefetividade do formato de contrato de adesão, tem-se a seguinte pesquisa:

Veja-se, a título de ilustração, o estudo empírico da Global Privacy Enforcement Network/GPEN que, por meio das suas 26 autoridades de garantia de proteção de dados pessoais<sup>157</sup>, constatou que, das políticas de privacidade de aplicativos móveis/mobile apps analisadas: i) 85% falham em prestar uma informação adequada sobre a coleta, o uso e o compartilhamento dos dados pessoais; ii) 59% são de difícil compreensão para extração de informações básicas a respeito de privacidade; iii) 1/3 está coletando dados pessoais excessivos e; iv) 43% têm uma

interface inadequada, seja porque a tela ou as letras são muito pequenas, seja porque se trata de longos textos que demandam a leitura de inúmeras páginas.<sup>95</sup>

Assim como estabelece o direito do consumidor, o excesso de informação gera a desinformação, e não o contrário. A estrutura dos termos de uso normalmente se mostra em textos longos, de linguagem complexa, algo que se mostra completamente oposto a dinâmica da sociedade da informação, que busca a velocidade e eficiência.

Da mesma forma que esta dinâmica se mostra essencial para as tecnologias da informação, elas impedem a viabilidade da proteção do consumidor através dos meios tradicionais. A lógica do sistema de proteção ao consumidor apresenta um controle *ex post*, onde, mediante a condição presumida de hipossuficiência do consumidor, o reequilíbrio da relação é almejado em juízo.

Todavia, os dados pessoais visam uma ideia *ex ante*, fornecendo previamente ao usuário o controle sobre suas informações, de forma que uma proteção posterior não seria eficiente a proteger o usuário.

Uma alternativa a ser pensada estaria focada em trazer esta massificação para os usuários também, onde eles pudessem acompanhar o trânsito de seus dados pessoais dentro do mercado informacional. Conforme Bruno Bioni explana, esta aplicação faz sentido pois envolve o mesmo objeto, os dados pessoais:

[...] Isso faz total sentido, pois, diferentemente, das relações ordinárias de consumo, essas (novas) relações são estruturadas universalmente sobre um mesmo “objeto de troca”: os dados pessoais, que são o trade-off desses novos modelos de negócios; ao contrário das relações off-line, em que a contrapartida de um bem de consumo é fixada, individual e pecuniariamente, para cada relação de consumo. Trata-se, pois, de perquirir se há novas formas de concretizar a prometida esfera de controle sobre os dados pessoais, se há novas ferramentas que sejam tão líquidas e fluidas quanto é o fluxo dos dados pessoais, e que percorram universalmente todo o ambiente on-line off-line das políticas de privacidade é uma ferramenta sólida que se presta para estaticamente exercer um controle dos dados para cada espaço e relação singular do ambiente eletrônico. É por tal razão, que esse ferramental não se ajusta à mencionada complexidade do fluxo informacional das renovadas relações de consumo, sobrecarregando o cidadão do século XXI.<sup>96</sup>

---

<sup>95</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2018, p. 172.

<sup>96</sup> BIONI, op. cit., p. 175.

Busca-se a partir desta ideia, perfazer o controle do usuário sobre seus dados informacionais, de maneira tão dinâmica quanto todo o ambiente online.

## 7.1 Tecnologias de Controle de Privacidade

Ao tempo que a tecnologia pode desempenhar o papel de vilã da privacidade, ela também é ferramenta essencial em prol da proteção dos dados pessoais.

Neste sentido, existem as *Privacy Enhancing Technologies/ PETs*<sup>97</sup>, que consistem em tecnologias que abarcam qualquer mecanismo de forma a torná-lo amigável à privacidade. Portanto, as *PETs* baseiam-se no conceito da proteção de dados orientar serviços e produtos, que devem conter tecnologias que proporcionem o melhor controle de informações pessoais.

São tecnologias que protegem princípios fundamentais de proteção de dados ao minimizar o uso de dados pessoais, maximizando a segurança de dados e empoderando indivíduos.<sup>98</sup>

Uma das *PETs* criadas foi chamada de *Do Not Track/ DNT*<sup>99</sup>, de modo que, na ideia do usuário em controle de seus dados pessoais, como este controle se daria, gerou discussões. A ideia desta ferramenta esteve concentrada na discussão entre se o usuário deveria consentir de forma prévia, devendo aceitar a cada navegação, se aceita que o cookie seja instalado ou não, ou se seria uma escolha configurada nos navegadores e cada site extrairia essa informação.

A escolha dos cookies autorizados manualmente foi uma das estratégias regulatórias apresentadas. Assim, passou-se a exigir o consentimento prévio e expresso dos usuários, que tiveram demasiados termos de autorização de instalação de cookies em inúmeros sites que acessavam.

Todavia, ao contrário do que se imaginava, o efeito gerado foi de tornar a experiência do usuário maçante, de forma que ocorria a rejeição ou aceite independente de compreender do que se tratava. A rigidez no procedimento do consentimento também foi falho em trazer controle ao usuário.

---

<sup>97</sup> Tecnologias de proteção à privacidade (tradução livre)

<sup>98</sup> TORRE, Lydia F. de La. What are Privacy-Enhancing Technologies (PETs)?. **Site Medium**. Disponível em: <https://medium.com/golden-data/what-are-privacy-enhancing-technologies-pets-8af6aea9923>. Acesso em 24 de out. 2019.

<sup>99</sup> Não rastreie (tradução livre)

É neste ponto que a DNT seria aplicada, sendo uma ferramenta que facilitaria o controle de dados, podendo ser um botão de Não Me Rastreie, onde automaticamente, o usuário poderia barrar ou permitir a coleta de dados. Seria um mecanismo atrelado aos navegadores, externalizando o consentimento do titular dos dados.

Poderia ser simplesmente uma forma do usuário controlar seus dados conforme sua preferência, sem que a experiência de navegação seja maçante com inúmeros pop-ups de cookies, e independente de conhecimento técnico do usuário.

É neste sentido que a doutrina entende:

De um lado, o consumidor não necessitaria ser um expert para deletar os vários trackers, a fim de vencer a corrida armamentista tecnológica de um rastreamento persistente. De outro lado, a sua experiência de navegação não seria prejudicada, já que tal tecnologia universalizaria a sua opção em não ter seus dados coletados por toda a web <sup>100</sup>

Embora muito interessante, a ferramenta teve sua implementação prejudicada pelo conflito entre atores que adjudicaram para si a padronização da DNT. Em meio a discussões entre a *World Wide Web Consortium* e entidades da indústria de publicidade comportamental, a tecnologia desta PET perdeu força, chegando a ser considerada apenas um mecanismo para não receber publicidade documental.

Além disso, houve conflito entre navegadores que anunciaram adotar o DNT como padrão, onde o usuário que desejasse ter seus dados coletados precisaria anuir expressamente, e o setor empresarial, que defendiam que a implementação da PET iria destruir a indústria da publicidade comportamental e as diversas aplicações derivadas dela.

Por fim, a ferramenta não foi implementada pela falta de consenso e padronização, ainda que alguns navegadores disponibilizem esta funcionalidade, não há garantia de que os provedores de aplicação irão respeitar o não rastreamento.

A DNT não possui força cogente e resta a vontade da indústria se autorregular para que ela venha a se concretizar. A trajetória de toda a PET destaca que o usuário depende de intervenção regulatória, não somente para prescrever o

---

<sup>100</sup>BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2018, p. 180.

seu direito à auto-regulamentação informacional, mas que, sobretudo, interfira para sua operacionalização. É ineficaz discutir se o consentimento deve ser prévio ou a posteriori se não há um movimento de regulação para efetivar esse direito.<sup>101</sup>

É neste sentido que os estudos se manifestam acerca da temática:

É que o estabelecimento de um regime de proteção de dados pessoais bem regulado, com todas as consequências que inevitavelmente implica, atinge centros de interesses bastante diversos, devendo existir necessariamente um esforço legislativo tal que resulte em uma sofisticação terminológica suficiente a dar conta de todas as contingências tecnológicas do debate que se trava<sup>102</sup>

Há também a ideia de granular o consentimento do usuário, configurando seu navegador para suas preferências de privacidade, como autorizar a coleta de dados sensíveis, não sensíveis, geolocalização e até compartilhamento com terceiros. De forma ao próprio navegador realizar uma análise automática dos termos de uso das aplicações, verificando a conformidade com as preferências selecionadas anteriormente.

O mecanismo que tornaria isto possível é denominado *Platform for Privacy Preferences*<sup>103</sup>, desenvolvida e recomendada pela World Wide Web Consortium. A ferramenta exigiria a alteração das aplicações para padronizar suas políticas de privacidade em formato que permita a leitura automatizada dos termos de uso.

Todavia, assim como a DNT, a sua efetivação restou falha pela ausência de regulamentação cogente que obrigasse os atores da internet a agir em estabelecer esta PET:

Com efeito, a P3P teria o potencial de tornar o fluxo informacional massificado para ambos os lados da relação de consumo do mercado informacional, já que tal tecnologia permitiria aos consumidores universalizar as suas preferências de privacidade e, conseqüentemente, controlar seus dados pessoais sem que fosse necessária a leitura singular e impraticável de cada política de privacidade. Dito de outra forma, a PET em questão empregaria fluidez à autodeterminação informacional, capilarizando-a frente à massa de relações travadas na economia digital pelo titular das informações. Mais do que isso, afastar-se-ia a lógica do

<sup>101</sup>BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro, 1. ed: Forense, 2018, p. 182.

<sup>102</sup> RUARO, Regina Linden, RODRIGUEZ, Daniel Pinero, FINGER, Brunize. **O Direito À Proteção De Dados Pessoais e a Privacidade Right To Personal Data Protection And The Privacy**. Revista da Faculdade de Direito - UFPR, Curitiba, n.47, p.29-64, 2008. Disponível em: <https://revistas.ufpr.br/direito/article/download/30768/19876>. Acesso em: 22 de out. 2019.

<sup>103</sup> Plataforma de preferências de privacidade (tradução livre)



“tudo” ou “nada” das políticas de privacidade, na medida em que o “concordo” ou “discordo” poderiam ser substituídos pela granularidade das autorizações especificadas nas preferências de privacidade. Assegurando-se tal poder de barganha na troca econômica (trade-off) da economia de dados, a P3P empoderaria o cidadão com uma autonomia genuína sobre o fluxo de suas informações pessoais. O leque de opções do processo de tomada de decisão avançaria para além da lógica binária do take-it ou leave-it<sup>104</sup>

Os cidadãos teriam desta forma, uma ferramenta para massificar o seu fluxo informacional, de forma que universalizaria suas preferências de privacidade ao tempo que não seria mais necessária a desgastante leitura de todos os termos individualmente.

Além disso, essa PET seria capaz de fragmentar o consentimento, trazendo um poder de barganha ao usuário, algo que se justifica por sua condição de consumidor que realiza “pagamento” por meio de seus dados pessoais, em troca do serviço ou produto oferecido pelo fornecedor.

Nesta relação, embora inicialmente pareça equilibrada, no momento que o usuário concede suas informações pessoais, ele perde o controle absoluto da destinação e uso que elas terão a partir de então, permitindo que um terceiro os controlem conforme seus interesses particulares.

O que se busca, portanto, é recuperar um poder ao titular dos dados pessoais, para que este exerça controle sobre o fluxo informacional que movimenta e tenha consciência acerca dos usos a que serão destinados.

Reza clara a contradição de interesses entre os sujeitos nesta relação, estando claro o protagonismo dos dados pessoais, onde uma parte busca explorá-los e outra almeja o controle sobre esta exploração.

Um dos princípios elencados pela LGPD dispõe a respeito da transparência, com informações claras, precisas e facilmente acessíveis. Além disso, elenca que o consentimento poderá ser considerado nulo caso não haja transparência.

Isto porque não se busca inverter a assimetria existente no mercado atual, e sim, reduzi-la, de modo que o usuário atual, que não possui poder algum sobre seus dados após consentir aos termos de privacidade, a ter uma relação menos obscura acerca do trajeto de seus dados pessoais. É neste sentido que a LGPD apresenta:

---

<sup>104</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2018, p. 183.

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:

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.<sup>105</sup>

Trata-se de caso onde a LGPD impôs que em situações onde o fornecimento de dados pessoais for necessário para o acesso de produto, serviço ou exercício de direito, o titular deverá ser informado sobre o consentimento e acerca de exercício de direito em situações como o acesso aos dados; eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.<sup>106</sup>

Isto pois a referida lei também é guiada pelo princípio da finalidade, estabelecendo ainda, que a finalidade deve ser respeitada, de modo a serem propósitos específicos, legítimos e explícitos ao seu titular, sem que haja tratamento posterior de forma incompatível com tais finalidades.<sup>107</sup>

Assim, todo tratamento de dados deve apresentar um fim específico e claro, pois todo consentimento deve ser direcionado, visualizando obter uma declaração de vontade inequívoca, seguindo as regras do direito civil brasileiro, que exigem que a manifestação de vontade seja livre e consciência, de modo que caso não seja, é considerado um vício de consentimento e torna-se negócio jurídico anulável.

Desta forma, a utilização de terminologias como “para melhorar a sua experiência”, comumente presente em termos de privacidade, deve ser abandonada, porque não atinge a finalidade precípua de efetivamente informar o usuário.

---

<sup>105</sup> BRASIL. Congresso Nacional. Lei nº 13.709, De 14 De Agosto De 2018. **Institui a Lei Geral de Proteção de Dados Pessoais**, Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709compilado.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm). Acesso em 16 de out. 2019.

<sup>106</sup> Art. 18 da LGPD

<sup>107</sup> Art. 6 da LGPD

Assim, uma possível mudança capaz de gerar maior equilíbrio nesta relação, segundo Bruno Bioni, seria:

Nesse sentido, uma das possíveis interpretações será analisar de que modo a configuração de serviços e produtos deve, por padrão, coletar a menor quantidade possível de dados. O titular dos dados seria estimulado a reconfigurá-las para fazer uso de determinadas funcionalidades, o que poderia ser visto como ação inequívoca da sua parte <sup>108</sup>

A tecnologia é onipresente, onde a arquitetura da rede foi projetada de modo que o controle não esteja dividido entre todos os usuários, mas sim, concentrado entre os fornecedores de serviços e produtos. Faz-se aqui, aplicação do código de defesa do consumidor, encaixando o usuário como situação de vulnerabilidade extrema.

Conforme apresentado, existem soluções que a tecnologia proporciona para que o usuário seja capaz de obter o controle acerca de seus dados pessoais, a controvérsia encontra-se na execução de tais medidas, uma vez que a ausência de intervenção regulatória impede a implementação delas.

A ideia de autorregulação do mercado comprovou-se falha, uma vez que dentro dele, existem inúmeros interesses controversos, os quais, sem a intervenção de uma ação regulatória do Estado, em que pese, busque a defesa de seus cidadãos, não será possível implementar medidas que sejam amigáveis aos usuários em busca de proporcioná-los controle acerca de seus dados pessoais perante sociedade em que as oportunidades que lhes são oferecidas, têm base neles.

## **7.2 A Autoridade Nacional de Proteção de Dados Pessoais (ANPD)**

A Lei Geral de Proteção de dados apresentou em seu projeto original a estruturação de uma Autoridade Nacional de Proteção de Dados, a qual foi inicialmente vetada pelo presidente. Com o advento da medida provisória 869 de dezembro de 2018, a LGPD foi alterada e a previsão da Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, foi estabelecida.

---

<sup>108</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2018, p. 200

A criação de uma autoridade independente, autônoma e com corpo técnico qualificado traz inúmeras benefícios a todos, sejam usuários ou empresas.

Além disso, inserida a visão do Poder Judiciário, a Autoridade, sendo independente e qualificada, impedirá que o tema fosse decidido de forma discrepante nas diversas instâncias que irão aplicar a lei, seja em nível federal, estadual ou municipal. Entre as funções delegadas a ela está a de uniformizar o cumprimento da lei, orientando a interpretação dos dispositivos legais.

A presença da autoridade implica especialmente que com o advento da lei, os cidadãos iniciarão a petição de demandas que envolvem os direitos trazidos pela LGPD chegando aos tribunais brasileiros, os quais irão apresentar os mais diversos entendimentos acerca do tema, uma vez que demanda conhecimento técnico específico.

Uma prática que vem sendo adotada por diversos países diz respeito à adequação de sua legislação nacional para aproveitar o desenvolvimento econômico proporcionado pela economia digital, além de ter segurança de seus dados e proteção da privacidade das pessoas naturais.

É neste sentido que a proposta para a criação da autoridade brasileira de proteção aos dados pessoais se manifesta acerca:

Uma maior compatibilidade entre os diferentes sistemas pode facilitar, por exemplo, os fluxos internacionais de dados, o que beneficiaria os mais diversos setores e poderia ser utilizado para fins variados, como comerciais e para a cooperação entre entidades públicas. Apenas a título exemplificativo, uma vez reconhecida a adequação do sistema de proteção de dados do Brasil pela Comissão da União Europeia, empresas portuguesas poderiam transferir seus call centers para o Brasil, já que a transferência internacional de dados entre Portugal e Brasil seria facilitada e não dependeria de maiores arranjos contratuais, como ocorre hoje em dia. O mesmo poderia acontecer com data centers ou mesmo provedores de computação na nuvem, já que as barreiras impostas pelo GDPR à transferência internacional de dados para países que não têm nível adequado de proteção de dados não se aplicariam ao Brasil, o que, como consequência, atrairia não apenas novos investimentos para o Brasil, mas também possibilidade de expansão dos negócios existentes, em razão da possibilidade de atender a todo o mercado da União Europeia.<sup>109</sup>

A implementação de uma autoridade no Brasil, preencherá um dos requisitos para que o Brasil seja reconhecido como adequado às normas impostas

---

<sup>109</sup> TEFFÉ, Chiara Apadaccini, VIOLA, Mário. **Instituto de Tecnologia & Sociedade do Rio**. Proposta para a Criação da Autoridade Brasileira de Proteção aos Dados Pessoais. Disponível em: <https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf>. Acesso em: 23 out. 2019.

pela GDPR, algo que na América do Sul, apenas Argentina e Uruguai tiveram a adequação reconhecida.

Dessa forma, a presença da autoridade nacional também será capaz de facilitar o ingresso do Brasil na Organização para Cooperação e Desenvolvimento Econômico (OCDE). Para que sejam inseridos, os países devem obrigar-se a cumprir as normas estabelecidas por eles, que incluem a proteção da privacidade e fluxos de dados.

No panorama geral, a autoridade será o órgão de fiscalização e aplicação da lei, tendo competência para analisar o tratamento de dados realizado por controladores e subcontratantes. Além disso, poderá impor punições quando necessário e atuará auxiliando os titulares de dados pessoais a terem acesso a informações claras, de modo a que tenham maior controle sobre suas informações.

Todavia, a autoridade foi inicialmente vetada na Lei nº 13.709/18 com base em fundamentos que questionavam as chances de vício da autoridade e questões orçamentárias.

A respeito do orçamento para a autoridade, levantou-se que não poderia criar gastos não previstos no orçamento, uma vez que sua implementação geraria custos, além disso, alegou-se a falta de competência do Poder Legislativo para criação de um órgão desta natureza. Assim, somente poderia ser feito pelo Poder Executivo, com base nos artigos 61, §1º e 37, XIX, da Constituição Federal.

O vício de autoridade foi levantado pelo Senado, isto justificado pela tese de que a primeira empresa que viesse a incorrer em sanção imposta por este órgão, alegaria sua inconstitucionalidade, desencadeando em insegurança jurídica e demanda ao Judiciário.

É necessário salientar que embora este tenha sido um dos argumentos utilizados em prol do veto, a previsão que a lei traz em seu art. 55, é no sentido estabelecer a autoridade como órgão regido pela Lei nº 9986/2000, pertencente à administração indireta. Desta forma, disporia de autonomia financeira e não haveria subordinação hierárquica. Logo, do ponto de vista prático, a autoridade seria capaz de fiscalizar tanto órgãos privados quanto públicos.

Neste diapasão, com o intuito de reforçar a independência, no projeto de lei ainda foram previstos mandatos distintos dos membros do Conselho Diretor da Autoridade com os de Presidente da República:

[..] previsão de mandatos com prazos distintos para os primeiros membros do Conselho Diretor da Autoridade — prazos esses não concomitantes com o de Presidente da República —, devendo eles gozar também de mandatos fixos e de estabilidade, disposições que visavam certamente limitar pressões políticas advindas do Governo Federal. A previsão de mandatos distintos impediria, por exemplo, que cada novo Presidente eleito modificasse toda a composição da agência durante o seu mandato e buscasse com isso determinadas facilidades<sup>110</sup>

Com a promulgação da lei, foi estabelecido que a ANPD será órgão pertencente à Presidência da República, podendo ser transformada em entidade autárquica no prazo de até 2 anos.

Conforme estabelecido, o conselho diretor da autoridade será composto por 5 diretores escolhidos pelo presidente da República. Neste quesito, a independência da autoridade vê-se comprometida.

Não somente isto, os cargos são indicados também pelo Presidente, e possuem natureza de comissão, e a demissão será possível como pena de processo disciplinar, sendo também competência dele a eventual exclusão do cargo.

A autoridade encontra-se regulada de maneira corrompida, cercada de interferência direta dos chefes do Poder Executivo: o presidente da República e o ministro chefe da Casa Civil. Considerando ainda, a abertura dada pelo uso da expressão “caso necessário”, implica na possibilidade de uma atuação discricionária.

Isto posto, embora haja previsão da LGPD em direção à autonomia técnica da Autoridade, em seu art. 55-B, a vinculação dela à administração direta do Poder Executivo, fazem com que exista vínculo de subordinação entre a autoridade e o poder público.

Além da referida autoridade, a lei 13.853 de julho de 2019, sancionada para regulamentar a criação da ANPD, trouxe ainda o Conselho Nacional de Proteção de Dados Pessoais e Privacidade, com mandato de 2 anos, composto por 23 membros representantes.

Entre a competência deste conselho estão previstos:

Ao conselho compete elaborar estudos, realizar debates e audiências públicas sobre proteção de dados pessoais e privacidade, disseminar conhecimento sobre estas áreas, entre outros. Ou seja, ele auxiliará a ANPD em suas funções, propondo ações a serem realizadas pela

---

<sup>110</sup> BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2018, p. 17

autoridade, além de atuar junto à sociedade, ao trazer informações e auxílio nos setores de proteção de dados e privacidade<sup>111</sup>

Em busca da melhor atuação da ANPD dentro do ordenamento jurídico brasileiro, tendo em vista seu caráter inédito aqui, o estudo acerca de sua atuação em outros países é capaz de proporcionar um melhor entendimento acerca do que deverá ser visado com sua implementação, e como maior referência, a aplicação do GDPR da União Europeia, vigente desde maio de 2018.

### 7.3 O Regulamento Geral Europeu de Proteção de Dados (GDPR)

A previsão de normas acerca da proteção de dados europeus está disposta no Regulamento Geral Europeu de Proteção de Dados. Uma destas previsões diz respeito a autoridades de controle independentes, sendo compreendidas como uma autoridade pública e independente, criada por um Estado-Membro.

A Autoridade Europeia para a Proteção de Dados (AEPD) tem como principal papel garantir que haja o respeito do direito à privacidade dos cidadãos da União Europeia por parte de suas instituições e organismos.

Sua criação data no ano de 2004, com sede na cidade de Bruxelas, na Bélgica. Sua organização se dá por meio de um supervisor chefe, um supervisor assistente, amparada por especialistas em tecnologia da informação, administradores e advogados. Atualmente, a supervisão geral encontra-se sob chefia de Giovanni Buttarelli, e Wojciech Wiewiórowski como supervisor assistente, ambos nomeados pelo Parlamento Europeu do Conselho, em dezembro de 2014, a fim de cumprirem um mandato de cinco anos.

Entre os princípios fundamentais da Autoridade, é notável o destaque à imparcialidade, pois a mesma deve ser objetiva e independente, de forma a trazer o equilíbrio às relações, uma vez que trabalha com o tratamento de dados dos cidadãos, desde sua coleta e registro, ao armazenamento e envio. A integridade de fazer o que seja correto, embora não seja popular.

---

<sup>111</sup> GARRUTE, Mateus Mello. SCHMIDT, Estela. **A autoridade nacional de proteção de dados e sua importância para os indivíduos e para o Brasil.** Disponível em: <https://www.migalhas.com.br/dePeso/16,MI307390,11049-A+autoridade+nacional+de+protecao+de+dados+e+sua+importancia+para+os>. Acesso em: 03 out. 2019.

Há ainda, a transparência, pois a Autoridade tem o dever de justificar o que faz e porquê o faz, de modo claro e acessível a todos. Conta ainda, que deverá estar atualizado das necessidades do mercado, buscando soluções práticas para as lides que eventualmente surgirem.

O objetivo da União Europeia ao instituir a Autoridade como órgão de excelência que traga eficiência prática para os padrões de privacidade e proteção de dados da União. Sua independência é constantemente ressaltada, pois é característica que proporciona credibilidade às decisões da instituição.

Entre as suas competências destacam-se: fornecimento de orientação para casos imprevistos dentro da proteção de dados; atuar em níveis complexos para criar uma comunidade com partes interessadas, integrantes da UE e não integrantes, organizações nacionais e internacionais, com o fim de intensificar as discussões acerca da proteção de dados; e de forma geral, em detrimento do seu corpo técnico especializado, propor recomendações e soluções práticas.

#### **7.4 Agência de Acesso à Informação Pública da Argentina**

O primeiro país da América Latina a ser reconhecido pela Comissão da União Europeia como adequado ao sistema de proteção de dados pessoais foi a Argentina.

De início, a autoridade competente para realizar a fiscalizar o cumprimento de sua lei de proteção de dados foi a *Dirección Nacional de Protección de Datos Personales*<sup>112</sup>, órgão cujo diretor somente poderia ser exonerado pelo Poder Executivo com base em mal desempenho de suas funções.

A ligação íntima da Direção com a administração direta foi criticada em relação à independência de sua atuação. De tal forma, em 2017, após o GDPR ser aprovado, a Direção passou a ser Agência de *Acceso a la Información Pública*.<sup>113</sup>

Esta, por sua vez, foi estabelecida em regime de autarquia, com as características de uma autoridade independente, pois passou a ter diretor com mandato estabelecido, corpo técnico e administrativo dedicado, além de completa autonomia funcional e financeira.

---

<sup>112</sup> Direção Nacional de Proteção de Dados (tradução livre)

<sup>113</sup> Agência de Acesso à Informação Pública (tradução livre)



As atribuições da Agência encontram-se estabelecidas na Lei nº 23.326/2000, a Lei de Proteção de Dados Pessoais da Argentina, em seu artigo 26.

114115

Por fim, é possível visualizar que a Argentina também optou por seguir o modelo europeu de autoridade independente para proteção de dados. Com a implementação da autoridade nacional no Brasil, certamente o fluxo de dados será impactado, pois o comércio e a cooperação internacional serão facilitados, diante de sua compatibilidade com a Argentina e também com o Uruguai, outro país que teve sua legislação reconhecida como adequada de acordo com o modelo europeu.

---

<sup>114</sup> ARTICULO 26.- (Prestación de servicios de información crediticia).

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

ARGENTINA. Ley 25.326. **Institui a lei de Proteccion De Los Datos Personales.** Disponível em: [https://www.oas.org/juridico/pdfs/arg\\_ley25326.pdf](https://www.oas.org/juridico/pdfs/arg_ley25326.pdf). Acesso em 23 de out. 2019.

<sup>115</sup> ARTIGO 26.- (Prestação de serviços de informação de crédito).

1. Na prestação de serviços de informações de crédito, apenas dados pessoais de natureza financeira relacionados à solvência e crédito financeiros, obtidos de fontes acessíveis ao público ou de informações fornecidas pela parte interessada com seu consentimento, podem ser processados.

2. Dados pessoais relacionados ao cumprimento ou violação de obrigações de conteúdo patrimonial, fornecidos pelo credor ou por qualquer pessoa agindo em seu próprio nome ou interesse, também podem ser processados.

3. A pedido do proprietário dos dados, o responsável ou usuário do banco de dados comunicará as informações, avaliações e avaliações que foram comunicadas sobre ele nos últimos seis meses e o nome e endereço do cessionário no caso de dados obtidos por transferência.

4. Somente dados pessoais significativos para avaliar a solvência econômico-financeira das pessoas afetadas durante os últimos cinco anos podem ser arquivados, registrados ou atribuídos. O prazo será reduzido para dois anos quando o devedor cancelar ou extinguir a obrigação, devendo esse fato ser registrado.

5. A prestação de serviços de informações de crédito não exigirá o consentimento prévio do proprietário dos dados para os fins de sua transferência, nem a subsequente comunicação dos dados, quando eles estiverem relacionados à transferência das atividades comerciais ou de crédito dos cessionários. (tradução livre)

## 7.5 Os Desafios da Aplicação Eficaz da LGPD no Brasil

A LGPD teve como base, um modelo europeu de proteção de dados. Embora na legislação brasileira seja algo um tanto quanto recente, na Europa teve início com as orientações da OCDE e a convenção 108 de Strasbourg, que datam no início da década de 1980.

Desde então, diversos instrumentos normativos foram utilizados para proporcionar maior eficiência ao tratamento de dados, incluindo o acompanhamento da evolução da sociedade da informação. O modelo europeu é muito rico, que evoluiu durante quatro décadas para chegar ao seu patamar atual, em oposição ao Brasil, que estabeleceu o prazo de 24 meses para a entrada em vigor da LGPD.

O período de 24 meses de *vacatio legis*, iniciados em 14 de agosto de 2018, em comparação a demais dispositivos legais, aparenta ser um prazo razoável, todavia, perante a realidade brasileira, nota-se que é um período muito curto, um grande desafio colocar em prática as normas estabelecidas pela LGPD, em especial, que, a um ano do fim deste período, sequer existe uma ANPD em andamento.

A base europeia mostra-se realmente sólida, sendo uma fonte de orientação capaz de direcionar o brasileiro diante das omissões que a LGPD apresenta, algo que deve ser tratado com muito cuidado para não criar uma “jabuticaba jurídica”, que comprometa todo o funcionamento da lei e seus principais objetivos.

Uma das peculiaridades que o sistema brasileiro apresentou trata da aplicação extraterritorial da lei. A título de exemplo, as companhias aéreas, ainda que não tenham filial no Brasil, mas que ofertem serviços a consumidores brasileiros, terão que respeitar as normas da LGPD.

Isto porque a lei será aplicada a quem efetuar qualquer tratamento de dados no Brasil, incluindo a finalidade de ofertar bens e serviços a pessoas no território brasileiro, e também quando tratar dados de indivíduos que estejam em território brasileiro, qualquer seja sua nacionalidade.

Isto posto, a atuação das companhias aéreas envolve muitos dados pessoais, como visto:

Além disso, companhias aéreas tratam muitos dados pessoais sensíveis, tais como verificação de identidade por biometria; dados de saúde do passageiro que demanda uma assistência específica durante o voo; e

dados a respeito de preferências alimentares que possam indicar convicção religiosa (como a alimentação *kosher*). Um maior cuidado com o tratamento de dados será necessário.

Ademais, passa a ser obrigatória a nomeação de encarregado pelo tratamento de dados pessoais, que terá as funções de atender pedidos dos titulares de dados pessoais, atuar perante a ANPD e estabelecer as diretrizes dentro da empresa para garantir a devida proteção de dados pessoais <sup>116</sup>

É necessário salientar que a LGPD, em seu artigo 52, inciso II, estabelece que os agentes que cometerem infrações, poderão receber multa de até 2% do faturamento da pessoa jurídica de direito privado, com o limite do total de 50 milhões de reais por infração.

A adequação à lei é algo que exige muito esforço, sob pena das empresas que não o fizerem, sofrerem danos, não somente econômicos, mas também à sua imagem de mercado, pois o uso indevido de dados pessoais vem ganhando cada vez maior potencial danoso.

A repercussão que uma lei de proteção de dados pessoais causa demonstra imensa relevância, não somente por seu objeto, mas também pela grandiosidade de sua aplicação. É capaz de afetar desde as empresas privadas de tecnologia até qualquer organização pública que realize o tratamento de dados.

O Brasil, por sua vez, não se mostra preparado para aplicar em todo o seu potencial a Lei Geral de Proteção de Dados. Após a entrada em vigor da lei, a Comissão de Proteção de Dados Europeia deverá decidir se o Brasil adequa-se aos seus parâmetros, e somente então poderá executar o seu potencial de ser destaque na América Latina, e poder ser inserido na crescente economia digital mundial.

---

<sup>116</sup> SATO, Luiza. BACCHINI, Mateus. **A Lei Geral de Proteção de Dados e os impactos nas companhias aéreas**, Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/a-lei-geral-de-protecao-de-dados-e-os-impactos-nas-companhias-aereas/>. Acesso em 16 de out. 2019.

## 8 CONCLUSÃO

O presente trabalho acadêmico buscou apresentar a sociedade da informação como o resultado das constantes evoluções tecnológicas, especialmente as que datam desde o período referente à Segunda Grande Guerra, especialmente a Internet, que nasceu como um projeto de pesquisa militar americano, o ARPA.

O referido projeto foi aperfeiçoado constantemente, até resultar na Rede Mundial de Computadores. E foi em torno dela que novas relações foram surgindo, pela sua dinamicidade e praticidade, substituiu o papel, superou barreiras geográficas e criou novas relações jurídicas.

A sociedade da informação se mostrou como a era do acesso, e não da propriedade. E diante dessas inovações, o direito, como ciência social, deve acompanhar a evolução, porque esta demanda um posicionamento jurídico que seja capaz de lidar com os riscos e benefícios que elas proporcionam.

A princípio, as redes são vistas de forma democrática, por seu acesso ser livre a todos os públicos, independente de requisitos objetivos. Com isto, novas empresas surgiram, de forma a agregar diferentes produtos e serviços ao mercado, como os serviços de streaming, como Youtube, Netflix, Spotify.

Todavia, a arquitetura dos meios digitais foge ao convencional, sendo necessário conhecimento técnico aprofundado acerca do tema. A estrutura da internet independe de um controle central, algo que proporciona ampla gama de utilização, mas também dificulta a responsabilização daqueles que abusem dela, já que a rede em si, não possui poder de controle de conteúdo.

Não somente as relações digitais são inovadoras ao sistema, como seus produtos e serviços. O modelo econômico tradicional é baseado na relação de compra e venda, o consumidor deve realizar o pagamento para adquirir ou usufruir de determinado serviço. Os negócios online são estruturados de forma que o pagamento não é requerido inicialmente.

Em contrário do que as relações comuns que não requerem pagamento, estes serviços não são gratuitos. Assim como todo empreendimento tradicional, os negócios online também requerem investimentos e visam a rentabilidade.

O que ocorre diante dos negócios online é resultado de sua estrutura ter sido montada de maneira que não requer o pagamento em espécie do usuário.

Todavia, isso se dá porque a plataforma, ao fornecer um serviço que já foi ou é concedido de forma gratuita, dificilmente conseguirá crescer de forma abundante realizando a cobrança por seus produtos.

Assim, meios alternativos de monetização foram buscados pelas empresas, especialmente as startups, e um deles foi a publicidade. À primeira vista, a sua relação com os dados pessoais parece distante, mas são eles a principal causa do sucesso da publicidade online.

Isto se dá devido ao fato dos usuários, ao concordarem com os termos de uso de uma plataforma, muitas vezes concedem o acesso aos seus dados e também de seus amigos na rede, como ocorre com o Facebook. Neste caso, a teia de alcance da rede torna-se maior, valorizando a rede e fazendo com que o serviço seja valorizado, sendo instrumento que analisa as informações concedidas por seus usuários e proporciona a publicidade direcionada.

Ao longo do tempo, a publicidade mostrou-se despersonalizada, com abordagens amplas, tendo como objetivo apenas alcançar o maior número de pessoas possível. Já com os serviços online, isto foi deixado de lado, pois ao analisar as informações de cada usuário, é possível auferir suas preferências e direcionar de forma específica, apenas as publicidades que se encontram dentro de sua alçada de público alvo.

O mercado evoluiu de forma a encontrar meios que lhe favoreçam agir com dispêndio de recursos mapeado a retornar com resultados mais efetivos. É o que se verifica com cada vez mais serviços de geolocalização, formas de extrair do usuário informações relevantes aos seus interesses. Não é à toa que as maiores empresas do mundo em questão de mercado informacional são as redes sociais.

Neste sentido, ainda que a abstenção regulatória seja uma forma interessante de permitir o livre desenvolvimento, caso ocorram atos atentatórios aos direitos da pessoa, a ausência de regulação específica pode resultar na omissão de tutela e gerar entendimentos jurisprudenciais divergentes, apresentando um ambiente caótico de insegurança jurídica.

Entre os direitos cuja tutela nos meios digitais merecem destaque estão o direito à privacidade, o direito de informação e o direito à proteção de dados. A privacidade, neste contexto, sempre foi muito ligada a um não fazer, ou seja, que terceiros não interfiram ou não tenham acesso a determinadas áreas ou informações de uma pessoa. O direito de informação é intimamente relacionado à estrutura das

redes, pois nele se baseia o direito de informar, expor dados, e ser informado, recebendo informações de forma livre.

Por último, temos o direito à proteção de dados. Diferentemente dos demais citados, não é um direito fundamental tutelado pela Constituição Federal Brasileira, mas sua natureza de direito da personalidade vem ganhando destaque na doutrina brasileira.

A sua relevância destaca-se por seu objeto estar diretamente ligado à commodity de maior valor na sociedade da informação: os dados informacionais. A proteção de dados pessoais não pode vincular-se a um instituto do direito comum, porque ele não pode ser classificado em nenhuma categoria específica.

Não há distinção entre esfera pública ou privada. Independe da vontade do usuário, um simples acesso, independente de tempo ou lugar, será registrado. É por meio deles que a economia da informação cresce exponencialmente, onde aqueles que a possuem em maior quantidade, têm um maior poder de controle, e conseqüentemente, maior conversão e monetização.

A coleta de dados com a formação de perfis e armazenamento em banco de dados é uma prática muito comum diante dos serviços online. Cada usuário possui um perfil na rede, formado por um aglomerado de informações que consideram desde registros pessoais ao seu comportamento na rede.

Neste diapasão, a ideia mais comumente difundida diz respeito a quais seriam as conseqüências da utilização dos dados de um usuário, pois, ainda que a tecnologia esteja intimamente presente na vida do indivíduo, é uma condição aparentemente distante da prática.

Isto não significa que a utilização deles não é realizada, mas que, em razão da hipossuficiência do usuário em relação aos seus dados pessoais. A falta de controle sobre os próprios dados resulta em uma inconsciência acerca da sua utilização.

É relevante salientar que os dados pessoais envolvem qualquer informação do usuário que esteja presente em um banco de dados, que seu uso pode ser particular, cedido especificamente a determinada empresa, mas que também é capaz de cedê-los a terceiros.

Por meio dessa dinamicidade, aquele que possui o poder de controle sobre os dados, tem o potencial de transformá-lo em ferramenta essencial para a finalidade que desejar, e neste ponto, o titular vê-se como figura vulnerável, podendo

ser utilizado pelo banco de dados da loja que analisa o perfil de consumo de cada cliente, enquadrando-o em uma categoria específica para direcionamento de ofertas, ocorrer a cessão de dados genéticos e até manipulação de informações em prol de um posicionamento político.

Existe no mundo digital, uma falsa sensação de controle por parte do usuário, quando na verdade, ocorre o exato oposto. Não existe nenhuma forma efetiva de proteção de dados atual, que efetivamente proporcione ao consumidor o poder de controle. Um dos meios mais utilizados atualmente se dá no modelo de contrato de adesão, através de termos de uso e privacidade. Não há que se discutir que se trata de um instrumento ineficaz na prática, pois o modelo de textos longos com linguagem complexa repele a sua leitura, além de ser uma abordagem incongruente com a dinâmica da internet.

O dado pessoal é um bem jurídico a ser tutelado, e sua importância deve ser destacada por instrumentos jurídicos que efetivamente propiciem ao seu titular, o controle sobre eles. Neste sentido, teríamos as tecnologias de controle de privacidade, que consistiriam em ferramentas a serem utilizadas pelos usuários através de seus dispositivos de acesso para terem o poder de apresentar um consentimento mitigado.

Todavia, sendo resultado de uma prática autorregulatória do mercado, houveram conflitos entre empresas que adjudicaram a competência de controlar essas ferramentas para si, fatos que enfraqueceram o movimento.

Os Estados, por sua vez, em destaque o Regulamento Geral de Proteção de Dados Europeu, passaram a regular o mérito, através da instituição de uma Autoridade que visa a proteção de dados. Neste sentido, o Brasil, através da Lei Geral de Proteção de Dados Pessoais, também instituiu uma Autoridade com os mesmos fins.

A LGPD ainda não se encontra em vigor no país, tendo sido instituído o prazo de *vacatio legis* equivalente a 24 meses, que terminará em agosto de 2020. A um ano do fim do prazo, o Brasil ainda não possui uma estrutura para abarcar todas as aplicações da lei, como a Autoridade, a um ano do término do prazo, não estará pronta para efetivar a aplicação da lei.

A efetiva proteção de dados pessoais no Brasil está em estágio primário, ainda que hajam previsões legais a respeito, a sua importância perante o

público geral ainda é abstrata, e ainda não consegue auferir sua real importância ao tratar de seus próprios dados.

A tutela destes dados será essencial para que haja equilíbrio nas relações concernentes ao direito digital, que em sua amplitude de aplicação, visa a proteção do usuário, de empresas privadas e instituições públicas, em prol do crescimento do Brasil no mercado informacional como potência da América Latina.



## REFERÊNCIAS

23andMe. Disponível em: <https://www.23andme.com/?myg=true>. Acesso em: 18 jul. 2019

**Agência Brasil**. O Celular se Torna a Principal Forma de Acesso à Internet no Brasil. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2018-07/celular-se-torna-principal-forma-de-acesso-internet-no-brasil>. Acesso em: 06 ago. 2019

ALAIMO, KARA. Mark Zuckerberg has lost all credibility with Congress - and the rest of us. **CNN, Estados Unidos**. Disponível em: <https://edition.cnn.com/2018/12/21/opinions/mark-zuckerberg-misled-congress-privacy-nyt-alaimo/index.html>. Acesso em 05 de ago. 2019

ALCANTARA, Larissa Kakizaki de. **Big Data e IoT: Desafios da Privacidade e da Proteção de Dados no Direito Digital**. 1. Ed. São Paulo: Independente, 2017. E-book.

ANDERSON, Chris. **Free! Why \$0,00 is The Future of Business**. Disponível em: <https://www.wired.com/2008/02/ff-free/>. Acesso em: 22 ago. 2019

BANSAL, Ankan, et al. **UMD Faces: An Annotated Face Dataset for Training Deep Networks**. Disponível em: <https://arxiv.org/abs/1611.01484>. Acesso em 17 ago. 2019.

BERNERS-LEE, Tim. **Weaving the Web: the original design and ultimate design of the World Wide Web by its inventor**. Nova York: HarperCollins Publishers, 2000.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2018.

Bit Definition. **Site Tech Terms**. Disponível em: <https://techterms.com/definition/bit>. Acesso em 28 fev. 2019.

BRASIL, Lei n. 10.406 de 10 de janeiro de 2002. **Institui o Código Civil**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/L10406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm). Acesso em 24 de abril 2019.

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

BRASIL. Congresso Nacional. Lei nº 13.709, De 14 De Agosto De 2018. **Institui a Lei Geral de Proteção de Dados Pessoais**, Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709compilado.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm). Acesso em 16 de out. 2019.

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

Encomendando uma pizza em 2010. **Site Devmedia**. Rio de Janeiro. Disponível em: <https://www.devmedia.com.br/forum/encomendando-uma-pizza-em-2010/125441>. Acesso em 09 de ago. 2019.

FADEYEV, Dmitri. **Uncompromising Design: Avoiding The Pitfalls of Free**". Disponível em: <http://www.smashingmagazine.com/2012/10/11/uncompromising-design-avoiding-pitfalls-free>. Acesso em: 22 ago. 2019.

FERREIRA, Ricardo Barretto, et al. **Site Migalhas**. Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia. <https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao>. Acesso em 22 de abril de 2019

GARATTONI, Bruno. 23andMe vai entregar DNA dos seus usuários para gigante farmacêutica. **Site Super Abril**. Disponível em: <https://super.abril.com.br/comportamento/23andme-vai-entregar-dna-dos-usuarios-para-gigante-farmaceutica/>. Acesso em: 20 de jul. 2019.

GARRUTE, Mateus Mello. SCHMIDT, Estela. **A autoridade nacional de proteção de dados e sua importância para os indivíduos e para o Brasil**. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI307390,11049-A+autoridade+nacional+de+protecao+de+dados+e+sua+importancia+para+os>. Acesso em: 03 out. 2019.

GOMES, Sílvia Maria; RODRIGUEZ, Carlos Manuel Taboada. **Configuração de cadeia de suprimentos**: estudos de casos em ambiente dinâmico de competição. Disponível em: [https://www.aedb.br/seget/arquivos/artigos08/164\\_164\\_seget.pdf](https://www.aedb.br/seget/arquivos/artigos08/164_164_seget.pdf). Acesso em: 28 fev. 2019.

HIRATA, Alessandro. **Enciclopédia Jurídica**. Direito à privacidade. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade>. Acesso em 30 mar. 2019.

LEMONS, Ronaldo et al. **Marco Civil da Internet**. São Paulo: Atlas, 2014

LEONARDI, Marcel. **Tutela e privacidade na internet**. 1. ed. São Paulo: Saraiva, 2012,

MAHDAWI, Arwa. **Is FaceApp an evil plot by 'the Russians' to steal your data?** Not quite. Disponível em: <https://www.theguardian.com/commentisfree/2019/jul/18/faceapp-privacy-data-russians>. Acesso em: 13 ago. 2019.

MARTINEAU, Paris. How to sign away the rights to your DNA. **Site The Outline**. Disponível em: <https://theoutline.com/post/5555/how-to-sign-away-the-rights-to-your-dna?zd=2&zi=rewxmeqw>. Acesso em 19 de jul. 2019.

MARTINI, Renato. **Sociedade da Informação** - para onde vamos. 1ª Ed. São Paulo: Trevisan, 2017. *E-book*.

MONTEIRO, Renato Leite. BIONI, Bruno. Que tal uma pizza de tofu com rabanetes? Você vai adorar!. **Huffpost**. Disponível em: [https://www.huffpostbrasil.com/renato-leite-monteiro/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar\\_a\\_21682549/](https://www.huffpostbrasil.com/renato-leite-monteiro/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar_a_21682549/). Acesso em 08 de ago. 2019.

MORAES, Amaro e NETO, Silva. **Falácia eletrônica**: a internet não criou um novo bem jurídico a ser tutelado. **CONJUR**. Disponível em: [https://www.conjur.com.br/2006-dez-06/internet\\_ao\\_criou\\_bem\\_juridico\\_tutelado](https://www.conjur.com.br/2006-dez-06/internet_ao_criou_bem_juridico_tutelado). Acesso em: 29 mar. 2019

PAESANI, Líliliana Minardi. **Direito e Internet**: Liberdade de Informação, Privacidade e Responsabilidade Civil, 7 ed. São Paulo: Atlas, 2014. e-book.

PEREIRA, José Matos. **Direito de Informação**. Lisboa: Associação Portuguesa de Informática, 1980.

PEREZ, Clotilde, BARBOSA, Ivan Santo. **Hiperpublicidade: fundamentos e interfaces**. v.1. São Paulo: Cengage Learning, 2017. E-book.

PIERCE, Justin. **USC Annenberg Digital Future Study Finds Strong Negative Reaction to Paying for Online Services**. Disponível em: <https://annenberg.usc.edu/2010-usc-annenberg-digital-future-study-finds-strong-negative-reaction-paying-online-services>. Acesso em 22 ago. 2019.

PINHEIRO, Patricia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2015. E-book

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais: comentários à Lei nº 13.709/18 (LGPD)**. São Paulo: Saraiva Educação, 2018

PORTUGAL. **Constituição da República Portuguesa**. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em 23 out. 2019.

PORTUGAL. **Convenção 108 Para A Protecção Das Pessoas Relativamente Ao Tratamento Automatizado De Dados De Carácter Pessoal**. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 21 abril 2019.

ROB, Peter. **Sistemas de Bancos de Dados: projeto e implementação**. Trad. All Tasks. São Paulo: Cengage Learning, 2011.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

ROSA, António Machuco. **As origens históricas da Internet: uma comparação com a origem dos meios clássicos de comunicação ponto a ponto**. Disponível em: <http://www.ec.ubi.pt/ec/11/pdf/EC11-2012Mai-05.pdf>. P 103. Acesso em: 28 mar. 2019

RUARO, Regina Linden, RODRIGUEZ, Daniel Pinero, FINGER, Brunize. **O Direito À Proteção De Dados Pessoais e a Privacidade Right To Personal Data Protection And The Privacy**. Revista da Faculdade de Direito - UFPR, Curitiba, n.47, p.29-64, 2008. Disponível em: <https://revistas.ufpr.br/direito/article/download/30768/19876>. Acesso em: 22 de out. 2019.

SATO, Luiza. BACCHINI, Mateus. **A Lei Geral de Proteção de Dados e os impactos nas companhias aéreas**, Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/a-lei-geral-de-protecao-de-dados-e-os-impactos-nas-companhias-aereas/>. Acesso em 16 de out. 2019.

SEBASTIAN, Kent. **No Such Thing as a Free Lunch: Consumer Contracts and "Free" Services**. Ottawa: Public Interest Advocacy Centre, 2014.

**Site CanalTech**. Agora é Oficial: Google compra Waze por US\$ 1,1 bilhão. Disponível em: <https://canaltech.com.br/mercado/Agora-e-oficial-Google-compra-Waze-por-US-11-bilhao/>. Acesso em: 8 ago. 2019.

STANLEY, J. Adrian. **UCCS secretly photographed students to advance facial recognition technology**. Disponível em: <https://www.csindy.com/coloradosprings/uccs-secretly-photographed-students-to-advance-facial-recognition-technology/Content?oid=19664437>. Acesso em 15 ago. 2019.

Stiglitz , Joseph E. **The revolution of information economics: the past and the future**. Disponível em: <https://www.nber.org/papers/w23780.pdf>. p. 4. Acesso em: 26 fev. 2019.

TEFFÉ, Chiara Apadaccini, VIOLA, Mário. **Instituto de Tecnologia & Sociedade do Rio**. Proposta para a Criação da Autoridade Brasileira de Proteção aos Dados Pessoais. Disponível em: <https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf>. Acesso em: 23 out. 2019.

**The Guardian**. Disponível em: <https://www.theguardian.com/uk-news/2018/mar/20/david-carroll-cambridge-analytica-uk-courts-us-professor>. Acesso em: 03 ago. 2019.

TORRES, Claudio. **A Bíblia do Marketing Digital**. 2. ed. São Paulo: Novatec, 2018. e-book

TORRE, Lydia F. de La. What are Privacy-Enhancing Technologies (PETs)? **Site Medium**. Disponível em: <https://medium.com/golden-data/what-are-privacy-enhancing-technologies-pets-8af6aea9923>. Acesso em 24 de out. 2019.