

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”  
FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS**

**FELIPE OTÁVIO MORAES ALVES**

**TUTELA ESTATAL DA INTERNET À LUZ DA TÉCNICA**

**FRANCA**

**2023**

**FELIPE OTÁVIO MORAES ALVES**

**TUTELA ESTATAL DA INTERNET À LUZ DA TÉCNICA**

Dissertação apresentada à Faculdade de Ciências Humanas e Sociais da Universidade Estadual Paulista “Júlio de Mesquita Filho” como pré-requisito para obtenção do título de Mestre em Direito. Área de concentração: Sistemas Normativos e Fundamentos da Cidadania.

Orientador: Prof. Dr. Jorge David Barrientos-Parra

**FRANCA**

**2023**

A474t      Alves, Felipe Otávio Moraes  
Tutela estatal da internet à luz da técnica / Felipe Otávio  
Moraes Alves. -- Franca, 2023  
216 f. : tabs.

Dissertação (mestrado) - Universidade Estadual Paulista  
(Unesp), Faculdade de Ciências Humanas e Sociais,  
Franca  
Orientador: Jorge David Barrientos-Parra

1. Direito. 2. Internet. 3. Estado. 4. Técnica. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da  
Faculdade de Ciências Humanas e Sociais, Franca. Dados fornecidos pelo  
autor(a).

Essa ficha não pode ser modificada.

**FELIPE OTÁVIO MORAES ALVES**

**TUTELA ESTATAL DA INTERNET À LUZ DA TÉCNICA**

**Dissertação apresentada à Faculdade de Ciências Humanas e Sociais da Universidade Estadual Paulista “Júlio de Mesquita Filho” como pré-requisito para obtenção do título de Mestre em Direito. Área de concentração: Sistemas Normativos e Fundamentos da Cidadania.**

**BANCA EXAMINADORA**

**Presidente:** Prof. Dr. Jorge David Barrientos-Parra

**1. Examinador:** Profa. Dra. Jete Jane Fiorati

**2. Examinador:** Prof. Dr. Fernando Pasquini Santos

**Franca, 12 de janeiro de 2023.**

Dedico o presente trabalho à minha família, pelo carinho e suporte durante toda minha experiência acadêmica. E por fim, porém não menos importante, à minha amada Paola Gomes Souza, por todo amor e suporte essenciais em meu trajeto acadêmico e profissional.

A seguir, dedico à Universidade Federal de Goiás (UFG), que consolidou e estimulou meu empenho, força e conhecimento conquistado para todas atividades acadêmicas realizadas, e à UNESP, por concretizar minha meta de me tornar mestre em uma universidade tão inspiradora.

## **AGRADECIMENTOS**

Agradeço aos meus professores que conduziram meus ensejos acadêmicos para os melhores caminhos. Como dita Friedrich Nietzsche, retribuímos mal a um professor se continuamos apenas alunos. Hoje, tenho a pretensão de me tornar docente perante tantos exemplos dos eméritos professores da vetusta Faculdade de Ciências Humanas e Sociais da UNESP.

Agradeço ao meu orientador, professor e doutor Jorge David Barrientos-Parra por me auxiliar na realização desse projeto e, sobretudo, na afinidade por grandes filósofos da tecnologia e sociólogos essenciais na cultura jurídica.

Muito obrigado a todos!

ALVES, Felipe Otávio Moraes. Tutela Estatal da Internet à Luz da Técnica. 2023. 216 f. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito, Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Franca, 2023.

## RESUMO

Este trabalho busca problematizar a responsabilidade dos Estados na proteção da internet, conciliando as críticas teóricas de Jacques Ellul sobre a técnica com casos práticos, mediante sua perspectiva de insuficiência técnico-jurídica na defesa dos direitos fundamentais no contexto da sociedade técnica hodierna. Assim, o problema central é estabelecer até que ponto deve o direito e o Estado ser eficaz, trazendo segurança ao cidadão-consumidor, em detrimento de sua liberdade – tão importante para Ellul – e privacidade, ou seja, estudar se existe algum limite, e qual é ele, à técnica informática que se impõe a custo da liberdade e da violação do direito à intimidade dos usuários. A conscientização da imponente do progresso técnico sobre a condição humana e das características intrínsecas da técnica devem ser alcançadas para a devida avaliação de seus efeitos na internet. Como método de abordagem, é utilizado o dedutivo. Utilizamos também o método dialético. E com o uso da lógica, costumes, bom senso e a moderação fático-lógica, deve-se alcançamos problematizações com a devida transparência, finalidade legítima e proporcionalidade. Foi concluído que o Direito tem que estar de acordo com a justiça e não deve enxergar o indivíduo dentro de uma racionalidade técnica.

**Palavras-chave:** direito; internet; estado; técnica.

ALVES, Felipe Otávio Moraes. Tutela Estatal da Internet à Luz da Técnica. 2023. 216 f. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito, Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Franca, 2023.

### ABSTRACT

This work seeks to problematize the responsibility of the States in relation to the protection of the internet, seeking to reconcile the theoretical criticisms of Jacques Ellul on the technique with practical cases, through his perspective of technique-legal insufficiency in the defense of fundamental rights in the context of the technical society today. Therefore, the main problem is to establish the extent to which the law and the State should be effective, bringing security to the citizen-consumer, to the detriment of their freedom – so important to Ellul – and privacy, that is, studying if there is any limit, and which is, to the technique that imposes itself at the cost of freedom and the violation of the users' right to privacy. Awareness of the imposition of technique's progress on the human condition and the intrinsic characteristics of the technique must be achieved in order to properly assess its effects in the internet. As a method of approach, the deductive method is used. We also use the dialectical method. And with the use of logic, customs, common sense and factual-logical moderation, we must reach problematizations with due transparency, legitimate purpose and proportionality. It was concluded that the Law has to be in accordance with justice and should not see the individual within a technical rationality.

State tutelage of the internet in the light of technique

**Keywords:** law; internet; state; technique.

## LISTA DE QUADROS E TABELA

|                                                                                                                                                                                                        |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| QUADRO 01 – Como o comportamento forma um estágio intermediário entre implicações sociais e a interação usuário-produto e, portanto, respectivamente, entre preocupações coletivas e individuais ..... | 48  |
| QUADRO 02 – Quatro tipos de influência baseadas nas dimensões de força e saliência.                                                                                                                    | 50  |
| TABELA 01 - Tabela de preço de dados na <i>deep web</i> .....                                                                                                                                          | 74  |
| QUADRO 03 – Ciclo vicioso da violação da privacidade de dados pessoais .....                                                                                                                           | 122 |

## LISTA DE ABREVIATURAS E SIGLAS

|         |                                                                       |
|---------|-----------------------------------------------------------------------|
| 5g      | Internet of Fifth Generation                                          |
| ABNT    | Associação Brasileira de Normas Técnicas                              |
| ads     | Advertisements                                                        |
| ANPD    | Agencia Nacional de Proteção de Dados                                 |
| apps    | Applicatives                                                          |
| ARPANET | Advanced Research Projects Agency Network                             |
| art.    | Artigo                                                                |
| CC      | Código Civil                                                          |
| CCTV    | Closed-Circuit Television                                             |
| C&C     | Comando e Controle                                                    |
| CD      | Compact Disc                                                          |
| CDC     | Código de Defesa do Consumidor                                        |
| CEO     | Chief Executive Officer                                               |
| CERT    | Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança |
| CF      | Constituição Federal                                                  |
| CIA     | Central Intelligence Agency                                           |
| CONAR   | Conselho Nacional de Autorregulamentação Publicitária                 |
| coord.  | Coordenador(es)                                                       |
| CPC     | Código de Processo Civil                                              |
| CPP     | Código de Processo Penal                                              |
| CPF     | Cadastro de Pessoas Físicas                                           |
| CPI     | Comissões Parlamentares de Inquérito                                  |
| Ctrl    | Control                                                               |
| DA      | Direito Autoral                                                       |
| DARPA   | Defense Advanced Research Projects Agency                             |
| Des.    | Desembargador                                                         |
| DF      | Distrito Federal                                                      |
| DNA     | Deoxyribonucleic Acid                                                 |
| DP      | Direito de Propriedade                                                |
| DPO     | Data Protection Officer                                               |
| ed.     | Editor(es)                                                            |

|        |                                                             |
|--------|-------------------------------------------------------------|
| et al. | Et aliae                                                    |
| etc.   | Et cetera                                                   |
| EUA    | Estados Unidos da América                                   |
| FBI    | Federal Bureau of Investigation                             |
| GDPR   | General Data Protection Regulation                          |
| GO     | Estado de Goiás                                             |
| GPL    | General Public License                                      |
| GNU    | GNU's Not Unix                                              |
| HC     | Habeas Corpus                                               |
| HPE    | Hewlett Packard Enterprise                                  |
| IA     | Inteligência Artificial                                     |
| ICP    | Internet Protocol Communications Platform                   |
| IDs    | Identities                                                  |
| inc.   | Inciso                                                      |
| INPI   | Instituto Nacional da Propriedade Industrial                |
| IoT    | Internet of Things                                          |
| IP     | Internet Protocol                                           |
| LDA    | Lei de Direitos Autorais                                    |
| LGPD   | Lei Geral de Proteção de Dados Pessoais                     |
| MEC    | Ministério da Educação                                      |
| MCI    | Marco Civil da Internet                                     |
| Min.   | Ministro                                                    |
| MIT    | Massachusetts Institute of Technology                       |
| MP     | Ministério Público                                          |
| n.     | Número                                                      |
| net    | Internet                                                    |
| NSA    | Agência de Segurança Nacional dos Estados Unidos da América |
| OCR    | Optical Character Recognition                               |
| ONG    | Organização não governamental                               |
| org.   | Organizador(es)                                             |
| P2P    | Peer-to-peer                                                |
| PCs    | Computadores                                                |
| pdf.   | Portable Document Format                                    |

|         |                                                             |
|---------|-------------------------------------------------------------|
| PF      | Polícia Federal                                             |
| PI      | Propriedade Industrial                                      |
| PIPA    | Protect Intellectual Property Act                           |
| PL      | Projeto de Lei                                              |
| PSDB    | Partido Social Democrata Brasileiro                         |
| PT      | Partido dos Trabalhadores                                   |
| Rel.    | Relator(a)                                                  |
| R\$     | Real Brasileiro                                             |
| RG      | Registro Geral                                              |
| SMS     | Serviço de Mensagens Curtas                                 |
| SOPA    | Stop Online Piracy Act                                      |
| STATNET | Suite of Software Packages for Statistical Network Analysis |
| STF     | Supremo Tribunal Federal                                    |
| STJ     | Superior Tribunal de Justiça                                |
| TCP     | Transmission Control Protocol                               |
| TI      | Tecnologia da Informação                                    |
| TJ      | Tribunal de Justiça                                         |
| TV      | Televisão                                                   |
| UE      | União Europeia                                              |
| UNESP   | Universidade Estadual Paulista “Júlio de Mesquita Filho”    |
| URLs    | Uniform Resource Locators                                   |
| USB     | Universal Serial Bus                                        |
| US\$    | United States’s Dollar                                      |
| v.g.    | Verbi gratia                                                |
| web     | Rede da Internet                                            |
| www     | World Wide Web                                              |

## SUMÁRIO

|                                                                                                                                                                          |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>INTRODUÇÃO .....</b>                                                                                                                                                  | <b>15</b>  |
| <b>CAPÍTULO 1 INTERNET À LUZ DA TÉCNICA .....</b>                                                                                                                        | <b>19</b>  |
| <b>1.1 FILOSOFIA DA TECNOLOGIA .....</b>                                                                                                                                 | <b>19</b>  |
| <b>1.2 TÉCNICA EM JACQUES ELLUL .....</b>                                                                                                                                | <b>20</b>  |
| 1.2.1 História do Homem Técnico .....                                                                                                                                    | 23         |
| 1.2.2 Técnicas Psicossociais do Homem e Sacralização da Técnica .....                                                                                                    | 26         |
| 1.2.3 Risco e Sofrimento no Estado .....                                                                                                                                 | 27         |
| 1.2.4 Características da Técnica .....                                                                                                                                   | 31         |
| <b>1.3 TECNOLOGIA: CONCEITUAÇÃO E INFLUÊNCIAS .....</b>                                                                                                                  | <b>39</b>  |
| 1.3.1 Ética na Tecnologia .....                                                                                                                                          | 42         |
| 1.3.2 Influências de Produtos nos Indivíduos .....                                                                                                                       | 47         |
| <b>1.4 INTERNET: EVOLUÇÃO HISTÓRICA E ATUAL REALIDADE .....</b>                                                                                                          | <b>55</b>  |
| 1.4.1 No Mundo e no Brasil .....                                                                                                                                         | 57         |
| 1.4.2 Insuficiência das Empresas .....                                                                                                                                   | 64         |
| 1.4.3 Monetização de Malwares .....                                                                                                                                      | 71         |
| <b>CAPÍTULO 2 ESTADO, DIREITO E INTERNET .....</b>                                                                                                                       | <b>76</b>  |
| <b>2.1 IMPRESCINDIBILIDADE ESTATAL .....</b>                                                                                                                             | <b>76</b>  |
| <b>2.2 DIREITO DIGITAL .....</b>                                                                                                                                         | <b>79</b>  |
| <b>2.3 CARACTERÍSTICAS JURÍDICAS DA INTERNET E DO MEIO DIGITAL .....</b>                                                                                                 | <b>87</b>  |
| 2.3.1 Falsa Sensação de Anonimato e de Impunidade na Rede .....                                                                                                          | 88         |
| 2.3.2 Eternalização de Condutas e Irreversibilidade do Dano .....                                                                                                        | 90         |
| 2.3.3 Superposição de Multiníveis de Responsabilidades dos Provedores .....                                                                                              | 93         |
| 2.3.4 Percividade das Provas de Cibercriminosos .....                                                                                                                    | 97         |
| 2.3.5 Desconfiança Generalizada .....                                                                                                                                    | 98         |
| 2.3.6 Internacionalização de Condutas .....                                                                                                                              | 100        |
| <b>2.4 DIREITO DIGITAL COMO DIREITO REGULATÓRIO .....</b>                                                                                                                | <b>101</b> |
| <b>CAPÍTULO 3 ANÁLISE DOS PRINCIPAIS DILEMAS PRÁTICOS E TÉCNICOS NA REDE .....</b>                                                                                       | <b>109</b> |
| <b>3.1 COLISÃO DE DIREITOS E PRINCÍPIOS: PRIVACIDADE, LIBERDADE DE EXPRESSÃO, LIBERDADE DE IMPRENSA, TUTELA DA AVERIGUAÇÃO DE INFORMAÇÕES E SEGURANÇA JURÍDICA .....</b> | <b>109</b> |
| 3.1.1 Dinamismo dos direitos humanos fundamentais na rede .....                                                                                                          | 115        |
| 3.1.2 Tratamento de Dados Pessoais .....                                                                                                                                 | 119        |

|                                                                                                                               |            |
|-------------------------------------------------------------------------------------------------------------------------------|------------|
| 3.1.2.1 <i>Consentimento Quase-Tácito</i> .....                                                                               | 125        |
| 3.1.2.2 <i>Término do Tratamento de Dados</i> .....                                                                           | 132        |
| 3.1.3 Busca e Apreensão sem Mandado Judicial .....                                                                            | 135        |
| 3.1.4 Propriedade Intelectual na Internet .....                                                                               | 141        |
| 3.1.5 Restrição Publicitária e Indisponibilização de Conteúdos .....                                                          | 152        |
| <b>3.2 TÉCNICA ELLULIANA NA INTERNET .....</b>                                                                                | <b>158</b> |
| 3.2.1 Sacralização da Imagem e Banalização Da Palavra .....                                                                   | 163        |
| 3.2.2 Propaganda e Publicidade como Alienadoras a Serviço da Técnica .....                                                    | 166        |
| 3.2.3 Tecnicificação e Massificação da Humanidade .....                                                                       | 169        |
| <b>3.3 GLOBALIZAÇÃO DA INTERNET, NECESSIDADE DE CONSTITUIÇÕES CIVIS<br/>TRANSNACIONAIS E PROBLEMAS TRANSFRONTEIRIÇOS.....</b> | <b>171</b> |
| <b>3.4 TRANSUMANISMO E FUTURO DO HUMANO TECNOLÓGICO .....</b>                                                                 | <b>176</b> |
| <b>3.5 COMO LIDAR COM A TÉCNICA .....</b>                                                                                     | <b>182</b> |
| 3.5.1 Ações Preventivas.....                                                                                                  | 182        |
| 3.5.2 Direito de Fazer Nada .....                                                                                             | 187        |
| 3.5.3 Sabotar a Técnica.....                                                                                                  | 190        |
| <b>CONSIDERAÇÕES FINAIS.....</b>                                                                                              | <b>196</b> |
| <b>REFERÊNCIAS.....</b>                                                                                                       | <b>199</b> |

## INTRODUÇÃO

A internet é a atual tecnologia de maior impacto nas atuais relações sociais e jurídicas. A constante interligação da comunicação global faz dela de uma só vez, ao mesmo tempo e em qualquer lugar do mundo um mecanismo de disseminação informacional. Como principal intermédio de interação entre indivíduos na sociedade, a internet traz uma série de conflitos jurídicos a serem analisados nesta dissertação. Em virtude da carência de maior tutela estatal, do cenário globalizado e da atuação do progresso técnico, faz-se imperativa a proteção do ser humano e de seus direitos fundamentais. Destarte, surge o tema a ser trabalhado. Estudaremos, portanto, a tutela do Estado sobre a internet e seus entes, sujeitos à técnica.

Até que ponto devemos favorecer privacidades e liberdades individuais em detrimento da segurança jurídica? Delitos como injúria, calúnia e difamação podem não sofrer retratações legais por proteções à privacidade ao mesmo tempo que empresas e Estados gerem arbitrariamente dados pessoais dos usuários sem seus consentimentos expressos e verdadeiramente livres. Os métodos empregados por Estados, cibercriminosos, empresas e usuários definem quem somos e como agimos, especialmente em nível inconsciente e cultural. É a técnica quem busca traçar nossos caminhos, induzindo-nos a sermos mais artificiais, inumanos e previsíveis.

O problema é tão universal que, nos debates atualmente travados nos Estados Unidos e na Europa sobre o tema, sobejam dúvidas sobre qual modelo regulatório é o mais adequado na preservação da internet como uma plataforma aberta, evitando-se ao mesmo tempo regulações rígidas e excessivamente intervencionistas. O tema não poderia ser mais atual e carente de reposta jurídica. Afinal, sem a real coercibilidade de normas e com a ineficácia das ferramentas de combate aos cibercrimes, não há vinculação das condutas ilícitas e tampouco há diminuição de práticas lesivas na rede. Já adiantamos que não há uma fórmula correta, em que cada problema cibernético pudesse ser inserido para ser resolvido. É necessário analisar cada caso e, defendendo os melhores interesses sociais, apontar qual seria o caminho menos prejudicial a nós humanos.

Todas as vezes que algo novo surgir na sociedade ter-se-á que criar um ramo novo do Direito para regrá-lo? Observaremos que dependerá de cada situação e que, no que tange à internet, não caberá uma desregulamentação do Estado. Ocasionalmente, a internet é um novo meio para a realização de velhos e relativos delitos, mas, em outras vezes, testemunha milhares de atos ilícitos puros a serem tutelados pela carência da sociedade técnica, surgindo a necessidade do Direito Digital. O presente trabalho buscará estabelecer as adequadas diretrizes

deste novo ordenamento jurídico. Diversos países, como a Inglaterra e os Estados Unidos, já possuem, em suas faculdades de Direito, centros de estudos sobre normas jurídicas e a internet. No Brasil, todavia, observa-se ainda os primeiros passos, como as disciplinas que envolvem parte da discussão sobre a internet, alguns grupos de estudo e cursos de pós-graduação destinados a este tema. A incidência do estudo de Filosofia da Tecnologia em faculdades é ainda menor. Ainda assim, tanto no Brasil como em outros países, a principal dificuldade é encontrar soluções eficientes perante a imperativa evolução técnica.

Nesta Era Digital, o instrumento de poder é a informação. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso a essa informação, muitas vezes em forma de dados pessoais. Deve-se, por conseguinte, lembrar que o Direito é a somatória de comportamento e interação social e hoje esses dois elementos estão mais dinâmicos do que nunca, demonstrando que uma rígida norma não terá eficaz aplicabilidade. Assim, este trabalho estudará esta dinâmica político-institucional da internet e da técnica, aos parâmetros da juridicidade, pela concretização da cidadania e dos direitos fundamentais dos cidadãos. Para esta análise, indispensável será a compreensão das transformações históricas do mundo e do homem e, posteriormente, do Estado e do seu papel nesta tutela à internet, especialmente no âmbito internacional. Analisaremos estas relações tão intrínsecas por forças técnico-sociais, a interação em multiníveis de direitos e suas extensões eficaciais. Promovendo críticas que tangem ao transumanismo e a justiça no ciberespaço, desenvolveremos um pensamento crítico-social sobre a instrumentalização dos usuários para o efetivo exercício da cidadania. Se é certo que o mercado e a técnica geram progresso, confortos e desenvolvimento, também é certo que geram exclusão, alienação e submissão do homem, comprometendo o conceito de ser humano livre.

O trabalho tem como objetivo geral analisar como se interagem estes valores morais e fundamentais no âmbito cibernético internacional, estudando as normas que regem o mercado e sua estreita correlação inevitável com a técnica, a fim de estabelecer até que ponto deve o Direito ser eficaz, trazendo segurança ao cidadão, em detrimento de sua liberdade e privacidade. Isto é, estudaremos a técnica informática que se impõe a custo da liberdade e da violação do direito à intimidade dos usuários. Especificamente, estudaremos: a análise da conjuntura de usuários e empresas na internet e dos principais agentes sociais, econômicos e políticos envolvidos no meio cibernético, bem como seus respectivos interesses e lógicas de atuação; a compreensão da realidade a partir da atuação do Estado; as ideias de Estado, política, desenvolvimento e meio ambiente humano; o progresso técnico, em especial nas obras de Jacques Ellul e as modificações as quais a técnica gera na sociedade; o impacto da técnica sobre

o ordenamento jurídico digital; a eficácia como um valor intrínseco da sociedade e como afeta a relação do Direito com a internet; e os critérios para as devidas adequações dos conflitos de direitos fundamentais, a partir do exame da legislação constitucional e infraconstitucional e críticas à técnica. Analisar-se-á a crítica da eficácia como valor na sociedade e no Direito concomitante à noção da técnica como instrumento de legitimação e distribuição de poder político. Verificaremos a contribuição do arcabouço jurídico e ético, nacional e internacional, para a crise de legitimidade da democracia e para o déficit democrático de efetividade da governança. Afinal, a política tem perdido força para a técnica. A institucionalização da eficácia como instrumento da racionalidade científica e a tecnicização do pensamento jurídico serão abordados na explicação do direito como uma técnica de controle social.

Como não existe uma oposição natural entre nós e a tecnologia, por uma diferença no espaço-tempo, nos apropriarmos dela e fazemos seu melhor uso. Por um pacote de bem-estar, o homem entrega tacitamente toda sua liberdade por certas facilidades, consumação e segurança. Esse progresso técnico implica necessariamente a perda da liberdade do indivíduo. Na hermenêutica elluliana, devemos desenvolver um pensamento crítico social de inversão da tendência técnica em prol da vida, da saúde e do meio ambiente equilibrado. A ciência jurídica, como aparelho do Estado, é responsável por impedir abusos à população, podendo este trabalho, assim, contribuir na tentativa de engendrar uma sociedade ética, justa e igualitária.

Este trabalho indicará caminhos para um futuro desejável e plausível de protegidos ciberusuários, hoje nossa maior faceta concomitante com sermos consumidores. No primeiro capítulo, trataremos sobre a internet à luz da técnica. No início, introduziremos o que é a Filosofia da Tecnologia, do que se trata a aludida técnica na visão do tecnofilósofo francês Jacques Ellul. Explicaremos a presença da técnica na História da humanidade, com seu domínio psicossocial e a sacralização da técnica, além do uso que fez o ser humano – ou a técnica? – do risco e do sofrimento na sociedade. Trataremos das doze características da técnica e traduziremos como ela passou a ser artefato ou tecnologia e quais são as atuais discussões sobre a ética na sua criação ou design. Por fim, explicaremos a insurgência da internet, seus problemas e como todos seus estes interrelacionam-se.

No segundo capítulo, trataremos do Direito como criação histórica e legítima do Estado. Logo, o Direito Digital é meio do Estado tutelar a internet, com o contexto brasileiro e internacional a serem expostos. A instrução das características jurídicas do meio digital será essencial na análise da tutela estatal no ciberespaço. Teremos complementarmente a perspectiva do Direito como intervencionismo (econômico) e, ao final, o Direito como técnica de controle social e como isto afeta o próprio Direito e o Estado.

E no terceiro capítulo, desenvolveremos os vícios oriundos da técnica, pela internet, nos Estados e indivíduos. Explicaremos como lida nosso ordenamento com os conflitos de direitos fundamentais e o famoso paradoxo do Estado ser uma força restritiva que garante liberdade. Abordaremos o tratamento de dados pessoais e como nos afeta, especialmente enquanto técnica, com seu quase-tácito consentimento. Complementarmente, exporemos o impacto da técnica sobre a economia digital e sobre a cultura cibernética. Tal cultura pauta-se na sacralização e simbolização da imagem e na banalização da palavra, tratados por Ellul. Uma emblemática técnica é a propaganda, alienadora do ser humano, de seus sentimentos e de sua psiqué. Uma potencial solução é a restrição publicitária. Esta consequência alienadora é denominada de tecnificação da humanidade, ao massificar a aparência e a personalidade psíquica. Analisaremos a instrumentalização da internet como ferramenta de consolidação de direitos fundamentais e a fragmentação da propriedade intelectual na internet e, uma de suas soluções, a busca e apreensão sem mandado judicial. Teremos a análise da internet como fenômeno global e conheceremos o lado mais futurístico a qual a internet e as tecnologias podem chegar: o transumanismo. Por fim, trataremos da possibilidade de se negar a técnica.

Este trabalho almeja ser uma referência teórica útil na problematização dos atuais entraves na internet, mesmo que, em alguns momentos, nossos pontos de vista sobre fatos e morais não tenham a mais neutra fundamentação. Por exemplo, dificilmente teremos a profundamente científica da psiquiatria ou da psicologia coletiva ou cognitiva comportamental quando avaliarmos os danos mentais que certa técnica causa em certo indivíduo. A experiência de fatos e reconhecimentos de causas e efeitos se distinguem para cada indivíduo. Ressalvados os equívocos oriundos de problemas de indução e dedução, este trabalho se esforçará para ser cientificamente honesto e completo.

Para a construção da presente dissertação, é adotado o método teórico dedutivo, com respaldo aos fundamentos da privacidade, intimidade e liberdade a serem aplicados ao Direito Digital. As dúvidas, problematizadas durante o trabalho, são elucidadas com apoio de doutrinadores, especialistas na área digital e dados oficiais de regiões. O referencial teórico será o de Jacques Ellul, mas também seremos críticos quanto a ele. E como trabalho de conclusão de uma pós-graduação de uma instituição pública, devendo satisfação a todos contribuintes brasileiros que permitiram esta possibilidade, vale-se da linguagem jurídica e filosófica tão somente enquanto úteis – pela inexistência de outra menos rebuscada – para a compreensão de nossas interpretações. Vamos conversar sobre o impacto da internet em todos nós?

## CAPÍTULO 1 INTERNET À LUZ DA TÉCNICA

### 1.1 FILOSOFIA DA TECNOLOGIA

*Coube à filosofia da tecnologia enxergar o impacto da tecnologia na cultura.*

Para entender a internet à luz da técnica, inicialmente precisamos entender a filosofia da tecnologia, a técnica elluliana e suas características, a tecnologia e o artefato, a história do homem perante a técnica, a ética na tecnologia e a situação real de todos entes na internet para, consequentemente, entendermos como a técnica e a internet se relacionam nos tempos pós-modernos e com o Direito.

Para Sellars (1962, p. 35, tradução nossa), filosofia é a tentativa de “entender como as coisas, no sentido mais amplo possível do termo, se combinam no sentido mais amplo possível” e se a tecnologia é uma das coisas que a sociedade contemporânea mais utiliza, então a filosofia não pode ignorá-la. Mitcham (1994, tradução nossa) chama esta filosofia preocupada com a tecnologia de “filosofia da tecnologia das humanidades”. Basicamente, a Filosofia da Tecnologia busca soluções epistemológicas para focar em dilemas cotidianos em continuidade com a filosofia da ciência e com outros campos da filosofia moderna, mas não com as ciências humanas e sociais (FRANSSEN; LOKHORST; VAN DE POEL, 2018), como o Direito. Portanto, não será tarefa fácil, apesar de necessário tentar, combinar estas duas espécies de ciências, com suas singulares interpretações sobre um mesmo fato, a fim de auferir conclusões unificadas.

A ciência e a tecnologia estão intimamente interligadas, mas os campos da filosofia da ciência e da filosofia da tecnologia possuem abordagens distintas. Coube à filosofia da tecnologia – e não à filosofia da ciência – enxergar o impacto da tecnologia na cultura e no cotidiano, porque a ciência afeta diretamente a sociedade. Notemos uma dificuldade em encontrar um técnico-cientista crítico sobre o uso de sua tecnologia e ainda mais raro encontrar algum que deixou de utilizá-la por algum valor moral. E o presente trabalho abordará mais uma tecnologia em específico, a internet. E um exemplo da filosofia da tecnologia, a que dedicaremos estudo nesta dissertação, é justamente o trabalho de Jacques Ellul, apesar deste poder ser classificado mais como um sociólogo. Esta surgiu na década de 1960 e pode ser chamada de analítica porque não se preocupa a priori com as relações entre tecnologia e sociedade, mas sim com a tecnologia em si. Somente depois da análise da tecnologia, se pode

depreender suas influências na sociedade. É primeiro Ellul (1964) quem reconhece na técnica fundamento dominante e único para a tecnologia.

## 1.2 TÉCNICA EM JACQUES ELLUL

*A técnica anestesia o homem para aderir nele o inumano.*

Para melhor entenderem este trabalho, devemos conhecer o que é este tão falado termo de Ellul. A palavra técnica em si tem a origem grega de *techne*, alusivo à *poiesis* (criação), que retrata a capacidade do homem de aprender e produzir. Quase confunde-se às noções de racionalidade, lógica ou inteligência. Já a técnica moderna é um “fazer humano” que exige estudos científicos e artefatos tecnológicos. Ou seja, ambas técnicas evocam experiências de acertos e erros para serem aprimoradas, porém a moderna necessita do conhecimento científico pré-adquirido e quase confunde-se à tecnologia (MOCELLIN, 2012). E, cada vez mais, o homem é influenciado pela técnica moderna ao buscar a garantia de maior comodidade e de menos trabalho, mas essa dependência humana da exploração técnica moderna sobre a natureza faz o homem ser dominado pela técnica (ELLUL, 1964).

Ellul prezava muito a liberdade, quase em mesma paixão que liberais, e se preocupava com a nossa liberdade de autodeterminarmo-nos. Para o autor, técnica não é só a tecnologia da máquina. A técnica aqui tratada é diferente de tecnologia ou máquina. A primeira é o fenômeno de que tudo deve ser o mais eficiente possível; e a segunda, o principal meio pelo qual o ser humano se faz eficiente. Similares, mas distintas:

Sempre que vemos a palavra tecnologia ou técnica, pensamos automaticamente em máquinas. De fato, geralmente pensamos em nosso mundo como um mundo de máquinas. [...] É a máquina que agora depende inteiramente da técnica, e a máquina representa apenas uma pequena parte da técnica. [...] A máquina já não é sequer o aspecto mais importante da técnica (embora seja talvez o mais espetacular); a técnica assumiu todas as atividades do homem, não apenas sua atividade produtiva. (ELLUL, 1964, p. 1-4, tradução nossa).

Técnica refere-se a qualquer complexo de meios padronizados para atingir um determinado resultado que converte o comportamento espontâneo e não-reflexivo em comportamento deliberado, racionalizado e com resultados previsíveis, padronizados e quantitativos. Como dito, a técnica não se resume aos artefatos que utilizamos, consiste também nos conhecimentos teóricos que possibilitam sua construção e funcionamento. A máquina nos ajuda a controlar a natureza, pelo reconhecimento dos padrões comportamentais e naturais que

prejudicavam a satisfação integral das necessidades básicas do humano, transformando a natureza em algo inanimado e controlável através da máquina sociável e interativa. E aqui temos um problema. A técnica constrói um mundo em que a tecnologia e ser eficiente são indispensáveis que dificilmente podemos voltar ao que éramos (ELLUL, 1964, p. 4). A técnica se adapta a tudo, conciliando-se ao espírito darwinista de que os sobreviventes são, geralmente, os melhores adaptadores (DARWIN, 1859). E ao adaptarmo-nos e integrar a máquina na sociedade e na natureza, desumanizamo-nos:

Os homens agora vivem em condições que são menos que humanas. Pense em nossas fábricas desumanizadas, nossos sentidos insatisfeitos, nossas mulheres trabalhadoras, nosso distanciamento da natureza. A vida em tal ambiente não tem sentido. Considere nosso transporte público, no qual o homem é menos importante que uma encomenda; nossos hospitais, nos quais ele é apenas um número. No entanto, chamamos isso de progresso. E o barulho, aquele monstro que nos espreita a cada hora da noite sem trégua. É inútil protestar contra o capitalismo. O capitalismo não criou nosso mundo; a máquina fez. [...] A técnica integra a máquina na sociedade, constrói o tipo de mundo de que a máquina precisa e introduz ordem onde o bater incoerente da maquinaria amontoa ruínas. [...] A técnica integra tudo. Evita choques e eventos sensacionalistas. O homem não está adaptado a um mundo de aço; a técnica o adapta a ela. Muda a disposição desse mundo cego para que o homem possa fazer parte dele sem esbarrar em suas arestas, sem a angústia de se entregar ao inumano. (ELLUL, 1964, p. 5-6, tradução nossa).

Para Ellul, a técnica mascara os problemas de sua dominação ao consolar o ser humano com funcionalidades complexas e perfeitas através da racionalidade que cessa as possibilidades de erro e, sem escolher para errar, o homem se angustiará menos, porque a técnica evita dramas e anestesia o homem para aderir nele o inumano e quando a técnica entra em todas as áreas da vida, incluindo a humana, deixa de ser externa ao homem e se torna sua própria substância (ELLUL, 1964, p. 6).

A operação da técnica moderna engloba todos trabalhos humanos, realizados através de certo método visando certo resultado e a procura pelos métodos mais eficazes é dividida pelo autor em duas intervenções essenciais: a do julgamento, de criar artificialmente – e o que o homem cria que não é artificial? – um objeto sem necessariamente imitar a natureza, e a da consciência, de prever e dispor de possibilidades mais eficazes além do mundo natural (ELLUL, 1964, p. 18-19). Assim, o fenômeno técnico está em todos os campos porque queremos sempre o mais eficaz meio. Para Ellul, não existe a possibilidade de escolha de outra técnica, se não a mais eficaz. Mesmo antes da técnica moderna, nas primeiras atividades do humano primitivo, havia técnica:

A atividade técnica é a atividade mais primitiva do homem. Existe a técnica da caça, da pesca, da coleta de alimentos; e depois de armas, roupas e construção. E aqui nos deparamos com um mistério. Qual a origem desta atividade? É um fenômeno que não admite explicação completa. Pela pesquisa paciente, encontram-se áreas de imitação, transições de uma forma técnica para outra, exemplos de penetração. Mas no fundo

há uma área fechada o fenômeno da invenção. Pode-se mostrar que a técnica é absorvida pela psicologia do homem e depende dessa psicologia e do que se chamou de motivação técnica. Mas não temos nenhuma explicação de como surgiu uma atividade que antes não existia. Como o homem passou a domesticar os animais, a escolher certas plantas para cultivar? A força motivadora, dizem-nos, era religiosa; e as primeiras plantas foram cultivadas com algum fim mágico em mente. Isso é provável, mas como foi feita a seleção? E como aconteceu que a maioria dessas plantas eram comestíveis? Como o homem veio a refinar os metais e fazer o bronze? Foi acaso, como diz a lenda da descoberta do vidro fenício? Esta obviamente não é a resposta. Fica-se com um enigma; e há algum sentido em enfatizar que existe aqui a mesma qualidade misteriosa que existe na aparência da própria vida. Cada operação primitiva do homem implica a superação de um abismo tão grande entre o instinto e o ato técnico que uma aura mística paira sobre todo o desenvolvimento subsequente. Nosso culto moderno à técnica deriva do culto ancestral do homem ao caráter misterioso e maravilhoso de sua própria obra. (ELLUL, 1964, p. 23, tradução nossa).

Assim, a técnica esteve sempre presente na história da humanidade, como no método neolítico de lascar pedra para melhor perfurar animais e rivais. A principal crítica de Ellul ao modo como o homem se submete à técnica é a perda do seu senso social e comunitário, de suas responsabilidades, das suas autonomias funcionais e das espontaneidades sociológicas (ELLUL, 1968, p. 128). Afinal, ele se interessava pelas necessidades imateriais do homem, como sua liberdade e sua autodeterminação. Ellul não foi um inimigo das técnicas e tecnologias, pois isso era tão absurdo como dizer que ele era contrário a uma avalanche de neve ou a um câncer. Ele sabia que a técnica produzia situações úteis, agradáveis e confortáveis.

Vejamos que técnica é o meio:

Se reconhecermos que o método que cada pessoa emprega para atingir um resultado é, de fato, sua técnica particular, surge o problema dos meios. Na verdade, a técnica nada mais é do que um meio e o conjunto dos meios. Isso, é claro, não diminui a importância do problema. Nossa civilização é antes de tudo uma civilização de meios; na realidade da vida moderna, parece que os meios são mais importantes do que os fins. Qualquer outra avaliação da situação é mero idealismo. (ELLUL, 1964, p. 19, tradução nossa).

E assim, Ellul observa que os meios se tornam mais importantes que os fins. Como exercício, você, leitor, se considera um técnico? O Jurista o é, pois, tem como técnica ou meio o uso interpretativo e eficiente de normas com o fim de alguma espécie de controle social através de uma decisão judicial, ele é o “engenheiro dos direitos da sociedade e do Estado”. Ellul se preocupa quando o controle jurídico-social é o meio para o fim da efetivação da justiça, pois, qual seria o limite deste meio que justifica tal fim? A técnica (jurídica) não se restringiria apenas a esta tão subjetiva finalidade (da justiça social).

### 1.2.1 História do Homem Técnico

*Parece haver uma seleção natural que favorece as forças de negação psicológica da crua realidade.*

A solução técnica requer mudança apenas nas técnicas das ciências, exigindo pouca alteração nos valores humanos. Por isso, é preciso certa coragem para se abdicar de benefícios e negar uma solução técnica desejada por outro motivo além de sua eficácia. Para Hardin (2011), a título de exemplo, a maioria das pessoas que se angustia sobre a superlotação do planeta tenta encontrar uma maneira de evitar seus males sem renunciar os privilégios que desfruta. Pensa que alguma técnica de agricultura resolverá tecnologicamente este entrave. Mas, para ele, o problema populacional não pode ser resolvido de forma técnica tão quanto ganhar um jogo de xadrez contra uma máquina.

Vimos que havia técnica desde as primeiras atividades do humano primitivo. Na História, nota-se que a ruína de civilizações, povos e indivíduos é o destino social advindo de cada um perseguir seu próprio interesse e liberdade, trazendo ruína a todos. Parece haver uma seleção natural que favorece as forças de negação psicológica da crua realidade, já que quanto mais alienado, mais eficaz será o indivíduo em sua especialização e menos tempo estará preocupando com problemas cotidianos, mesmo que sofra a sociedade como todo. No âmbito ambiental, por exemplo, o ser humano está preso em um sistema de “sujar seu próprio ninho”, sem se preocupar com impacto à humanidade e às gerações futuras. Para Hardin (2011), é um erro pensar que podemos controlar a reprodução da humanidade ou os impactos ambientais a longo prazo por um apelo à consciência. E até o presente momento, esta realidade se confirma. Estimular o sentimento de medo da escassez à nível da Cidade do Cabo – em 1 ano, eles conseguiram grandes mudanças de comportamento quanto à economia de água, reduzindo pela metade a demanda apenas pela mudança de hábitos –, cuja água encontra-se perto de acabar, é o grande desafio dos ambientalistas. A longo prazo, o ineficaz apelo à consciência coletiva deve ser suficiente para condenar a humanidade, mas tem severas desvantagens de curto prazo também. Teorizando uma solução, retrata ele como seria o tratamento de um ser humano que resigna “em nome da consciência”: se não faz o que lhe é pedido, o homem é condenado por não ser cidadão responsável, é um desempregado vagabundo ou inútil pois não consegue modificar eficientemente toda a sociedade; já se se comporta, como lhe é pedido e imposto, o condenam como um simplório ou alienado enquanto o resto explora o que é comum (HARDIN,

2011). Todo homem crítico tem este duplo vínculo contraditório e não há posição confortável perante à técnica.

Na História, a retórica empregada para provocar obediência à coordenação social foi sempre a projeção do sentimento de culpa em não cooperadores. Essa mesma técnica humana sofreu mutações históricas tão somente em suas denominações. Esta culpa é produzida artificialmente pelo próprio homem a fim de gerar responsabilizações que criam uma coerção socialmente aceita, como nos padrões de beleza. É artificial pois não o homem não nasce com esta coordenação cooperativa em seus instintos e lhe é imposta, como podemos observá-la até em conjuntos de outros animais para adequar jovens ou novos integrantes ao comportamento daquele bando. O único tipo de coerção que o tecnofilósofo e sociólogo francês recomenda é a coerção mútua acordada pela maioria das pessoas afetadas, levando a outras séries de problemas práticos conhecido pelos Contratualistas. Mesmo que seja maléfico para si próprio, o ser humano se autossabota em crer sem se indagar que tais coerções são para um bem comum, como os tributos. Justamente porque a injustiça é preferível à teórica ruína total pelo descontrole social. Ao longo da História, este sempre fora o discurso: o prejuízo que tal sociedade passa é passageiro – como os períodos ditatoriais de Roma – e, futuramente, será causa de sucessos e benefícios. É o mal que valerá a pena um dia, esperam os controladores proféticos de todos povos, figura que ultimamente concentra-se em políticos e líderes religiosos. Tal discurso é uma das particularidades da guerra entre a reforma e o *status quo*, do querer mudar ou continuar como está. Ludicamente, o canal de YouTube “Porta dos Fundos” publicou o vídeo “Desprotesto”, no dia 26 de agosto de 2019, fazendo uma alegoria ao ridicularizar como seria uma manifestação popular em defesa de deixar a sociedade da forma em que já se encontra, protestando em desfavor de qualquer mudança. Uma medida de mudança é sempre derrotada quando os defensores triunfantes do “deixar como está” descobrirem na reforma uma mínima falha teórica e implicar que nenhuma mudança é possível sem um acordo unânime. A negação da realidade é tendência – quase uma adaptação darwiniana – histórica. Adoradores do *status quo* pressupõem que a realidade já é a melhor possível ou que a reforma proposta é imperfeita e deve-se aguardar uma proposta melhor.

Vejamos que a eficácia de uma determinada técnica é medida a partir da sua capacidade de ser aplicada ao homem sem gerar protestos. Inclusive esta é a definição da eficácia de uma norma jurídica: sua aptidão para produzir os efeitos desejados quando ajustada às necessidades e finalidades sociais do grupo. Basicamente, uma norma é mais eficaz na direta proporção que é mais aceita e menos desobedecida pelo povo. Logo, até a técnica jurídica incentiva a submissão acrítica do homem. Já na ciência-técnica, o pensador francês se preocupa que o

discurso científico universalizante – de tudo ser para o bem maior – é suficiente motivo de conforto e a finalidade da felicidade e saúde do ser humano constitui resposta padrão para qualquer questionamento, permitindo que o conhecimento tecnicocientífico continue a ser produzido sem entraves (ELLUL, 1964, p. 398). Um exemplo desta alienação nos problemas do Direito Digital é o automático reconhecimento dos benefícios da colheita de informações pessoais, muitas vezes por *cookies*, arquivos de internet que armazenam temporariamente as ações e informações do usuário na rede, para uma experiência diferenciada e específica para cada usuário. Clicamos em “Concordo” sobre o uso de cookies de uma página ou aplicativo, e dali em diante, nossas informações e dados são reproduzidos e compartilhados sem problemas.

A inevitabilidade do progresso técnico gera a desresponsabilização humana, já que não há uma consciência nesta dinâmica homem-técnica e, assim, ser humano é vítima do mundo. Torna-se muito comum este sentimento quando ocorre qualquer fato contrário à vontade humana. Se um computador tem problema, a culpa é do hardware; se a bolsa de valores entra em colapso, como em 2008, a culpa é das hipotecas sem fundo; se uma barragem se rompe ou há alagamentos em cidades, matando centenas, é culpa da natureza e/ou da engenharia da construção ou da falta de conhecimento dos técnicos de inspeção; se há aquecimento global, a culpa é dos automóveis e da indústria; se há guerra, é consequência fatal da presença de petróleo ou da ditadura daquele país; se há pobreza, a culpa são dos ricos, da exploração, da mais-valia ou do Capitalismo; se o homem erra no trabalho, a culpa é da falta de supervisão ou de conhecimentos não passados por outro responsável-superior; se o homem maltrata o próprio, a culpa é de sua criação familiar, de uma questão hormonal ou de alguma doença mental; se o homem rouba ou mata, é culpa de uma consequência social ou do meio o qual estava inserido, em que foi ele uma mera vítima do meio que estava inserido; se erra, culpa até deuses ou o “coitado do diabo”. Todos problemas são consequências naturais de outro fato, evento ou técnica, mas nunca dos humanos que as detêm ou executam. Cada vez mais, discursos de responsabilizações têm elementos e substantivos do cotidiano, mas nunca o humano em si. É culpa de tudo, menos de si próprio. O homem se dissocia até de sua mentalidade e a culpa, se eximindo, separando a mente, a perversa, do homem-vítima em si e de suas atitudes. Como se não tivéssemos controle mais do que somos ou fazemos e, assim, a técnica nos afasta de nossa mentalidade.

Desde cedo, a dissociação do homem de sua psique o desresponsabiliza pois ele não consegue mais ser crítico e agir em desfavor daquilo que o define. As crianças no mundo contemporâneo já pulam a fase da criatividade, pois as imagens-informações já estão prontas e, sem instigar um processo de criação ou crítica, elas só copiam ou aceitam o que lhe é dado. E

sem crítica e responsabilização, o homem se condena... Em nossa História, quando o ser humano assumiu, assume ou assumirá sua responsabilidade perante sua liberdade e sua noção de justo e verdadeiro?

### 1.2.2 Técnicas Psicossociais do Homem e Sacralização da Técnica

*A tecnologia nos faz agir com reflexo e não refletir.*

Quando refletimos sobre as técnicas, cremos que são as empregadas pelo homem, mas, na verdade, são aquelas empregadas no homem. Vejamos que o ser humano se expõe a um trabalho ligado ao tempo e ao custo-benefício da produção. Ellul aponta três instâncias da vida humana modificadas pelas técnicas: a modificação do meio e do espaço, a modificação do tempo e do movimento e, por último, a massificação da sociedade.

Sobre a primeira instância, o novo ambiente artificial criado pela máquina não foi feito para o homem e, por isso, modificou sua essência, seus meios de vida e seus hábitos:

Ele deve se adaptar, como se o mundo fosse novo, a um universo para o qual não foi criado. Ele foi feito para andar seis quilômetros por hora, e ele anda mil. Ele foi feito para comer quando estava com fome e para dormir quando estava com sono; em vez disso, ele obedece a um relógio. Ele foi feito para ter contato com os seres vivos e vive em um mundo de pedra. Ele foi criado com uma certa unidade essencial e é fragmentado por todas as forças do mundo moderno. (ELLUL, 1964, p. 325, tradução nossa).

Em relação à modificação do tempo e do movimento, o tempo da vida tornou-se mensurada pela máquina; em vez de viver nele, o homem foi dividido pelo tempo técnico, determinando ao homem quando comer, trabalhar, dormir, ter lazer, enfim, viver:

Comer, trabalhar e dormir estavam à disposição das máquinas. O tempo, que havia sido a medida das sequências orgânicas, foi quebrado e dissociado. A vida humana deixou de ser um conjunto, um todo, para se tornar um conjunto desconexo de atividades que não tinham outro vínculo senão o fato de serem realizadas pelo mesmo indivíduo. A abstração mecânica e a rigidez permeavam toda a estrutura do ser. O tempo abstrato tornou-se um novo meio, uma nova estrutura de existência. (ELLUL, 1964, p. 329, tradução nossa).

E a técnica condena o homem a um processo de massificação, sem que este saiba o que está acontecendo, o fazendo perder grande parte de sua individualidade porque ele não pode ficar muito tempo em desacordo com seu meio:

O processo de massificação ocorre não porque o homem de hoje seja por natureza um homem de massa, mas por razões técnicas. O homem torna-se um homem-massa no

novos quadros que lhe é imposto porque não consegue permanecer por muito tempo em desacordo com seu meio. A adaptação dos homens a uma sociedade de massas ainda não é um fato consumado; e pesquisas recentes no campo da sociologia psicanalítica revelaram a lacuna que ainda existe entre o homem e a sociedade coletiva, uma lacuna que é a causa do desequilíbrio. Toda sociedade tem normas que representam um critério do normal. Quando essas normas mudam de caráter, ocorre uma perturbação do equilíbrio e, para o homem que não acompanhou as mudanças, a neurose. Não há dúvida de que as normas de nossa civilização mudaram por razões que não são ‘humanas’; os homens como um todo não desejavam as mudanças ocorridas nem trabalhavam para elas conscientemente. (ELLUL, 1964, p. 332-333, tradução nossa).

Na domesticação do ser humano, seu criador inicial, este é obrigado a ser eficaz em detrimento da ação carregada de subjetividade e julgamentos, caso contrário sofrerá punições morais e sociais. Assim, o ser humano sacraliza a técnica e tudo que é eficiente. E Ellul entende ser sagrado ou sacralizado tudo aquilo que se decide inconscientemente respeitar e aceitar sem questionamentos e sua preocupação é essa submissão inquestionável que aceita os aspectos ruins destes entraves técnicos que o dominam, ou seja, ele se preocupa com a sacralização da técnica. Notemos que as pessoas se sentem mais seguras se forem ativamente controladas. Controle este que aliena horas, energia, eficiência e até sentimentos. A tecnologia nos faz agir com reflexo e não refletir. Pessoas aprendem a evitar riscos e as que não podem ser felizes na sociedade confortável devem sofrer de algum problema psicológico, pois a moral de hoje é da impossibilidade não ser feliz com tanto conforto, diversão compensatória, facilidades, consumação e segurança. Se um homem tenta ser mais individualista ou crítico, é ainda mais excluído de sua sociedade, pois é tratado como egoísta, restando a ele adaptar-se à dinâmica social que lhe é imposta.

### **1.2.3 Risco e Sofrimento no Estado**

*A ideia de segurança substitui a finalidade de justiça.*

Observemos o uso do risco e do sofrimento na História da humanidade. O que muda, durante seu percurso, foi o modo de explicar e evitar acontecimentos indesejados. Hodiernamente, o raciocínio técnico, de fim à eficácia, mesmo sem projetos para o futuro, parece ser o único regente das decisões humanas. E a noção de risco é um de seus fatores essenciais. A técnica e o conhecimento científico impõem que conheçamos a causa e evitemos o seu desencadeamento desastroso. Esse raciocínio valoriza a prevenção e a adoção de estilos

de vida que diminuam a probabilidade dos riscos, geralmente sinônimos de restrições de liberdades para maiores seguranças sociais.

A atribuição de responsabilidade normalmente liga o sofrimento a uma falha humana, a uma negligência. Há a crença de que, para todos os casos possíveis, existe uma técnica capaz de evitar aquele evento e, ainda mais, se o erro acontece, há algum humano a ser culpado. Isto gera uma transferência, do indivíduo vitimizado, de parte da sua responsabilidade sempre a outro. A técnica impõe que este indivíduo não se responsabilize tanto por seus atos para melhor dominá-lo, seja em forma de cultura, de Estado ou de trabalho. Um humano que se responsabiliza demasiadamente sobre seus atos é um ser mais difícil de ser manipulado pela técnica, pois tem mais autoconsciência. Esse raciocínio também explica a aceitação da violência aplicada pela polícia e do uso de técnicas cada vez mais invasivas para vigilância digital, objetivando a prevenção de eventos que geram sofrimentos coletivos. Não parece haver uma tendência de menor controle social sobre o indivíduo perante os riscos, que sempre serão justificativas para termos maior controle não só pelo Estado, mas por todos entes sociais. O Estado passa, então, a ser um gestor dos riscos, de quem se cobra tão somente que seja eficaz. O mundo se assustou e indignou-se com as denúncias do Snowden feita aos jornais de que o programa de vigilância PRISM dos Estados Unidos vinha sendo usado para espionar cidadãos do mundo todo. Edward Snowden era analista de inteligência junto à CIA e a NSA e denunciou as atividades de espionagem em junho de 2013. Já os americanos, pelo contrário, ainda detêm a ideologia de que se a pessoa tem nada a esconder, não há porque impedir o Estado de checar. Com a clássica visão humana de quem “não deve, não teme”, hoje a exploração destas vigilâncias americanas continua a mesma, senão até maiores. A China também tem adotado diversas medidas de controle social e até de ranqueamento através do mapeamento facial.

Para Ellul e para o presente autor, resta bem claro esse paradoxo em que o aperfeiçoamento dos métodos técnicos da polícia aumenta o controle sobre a sociedade a fim de protegê-la cada vez mais de criminosos. O autor francês se preocupa que este instrumento de controle tende a ser aplicado sempre e sem discriminação:

Quanto mais avançarmos, mais a polícia será responsabilizada pela reeducação dos desajustados sociais, objetivo que faz parte da própria ordem que lhes compete proteger. Estamos experimentando no momento a justificação desse desenvolvimento. Não é verdade que o aperfeiçoamento do poder de polícia seja fruto do maquiavelismo do Estado ou de alguma influência transitória. Toda a estrutura da sociedade o implica, necessariamente. Quanto mais mobilizamos as forças da natureza, mais devemos mobilizar os homens e mais exigimos a ordem, que hoje representa o valor mais alto. Negar isso é negar todo o curso dos tempos modernos. Esta ordem não tem nada de espontâneo. É antes um acréscimo paciente de mil detalhes técnicos. E cada um de nós sente segurança em cada uma das melhorias que tornam esta ordem mais eficiente e o futuro mais seguro. O pedido recebe nossa total aprovação; mesmo quando somos hostis à polícia, somos, por uma estranha contradição, partidários da ordem. No

desabrochar das descobertas modernas e do nosso próprio poder, uma vertigem se apoderou de nós e nos faz sentir essa necessidade em grau extremo. Afinal, é à polícia que cabe, do ponto de vista externo, zelar por essa ordem que abrange a organização e a moral. Como, então, podemos negar à polícia melhorias indispensáveis em seus métodos? (ELLUL, 1964, p. 102-103, tradução nossa).

As consequências desse processo são devastadoras para o Estado de Direito, pois as técnicas policiais transformam a nação em campo de concentração ou em uma constante quarentena. Vemos isto na internet e notemos que, majoritariamente, não é uma decisão perversa de um específico partido ou governo. Para todos eles, para estarmos seguros de (ciber)criminosos, é preciso que todos sejamos vigiados. A política moderna utiliza medidas excepcionais o tempo todo para garantir a manutenção da ordem e do combate a ameaças as quais colocam em risco o Estado. No Brasil, normativamente, evitamos esta unificação através do sistema de Freios e Contrapesos, pela superposição de poderes nos ditames da Constituição Federal. O estado de exceção é, então, a forma jurídica do controle político promovido pelos meios técnico. As populações mais afetadas pelas mazelas socioeconômicas passam de vítima da sociedade desigual para ameaçadora da ordem, pois tornam-se cidadãos que podem simultaneamente sofrer e cometer ações criminosas. E, na lógica da prevenção, é melhor manter distante a ameaça destes potenciais criminosos, mesmo que ainda não tenham agido. Dessa forma, a maior parte da população pobre de qualquer país é objeto de injustificadas prisões e são vítimas do *modus operandi* das forças policiais, legitimadas pelos discursos das classes média e alta que requerem a intervenção do Estado para a contenção de riscos vinculada ao risco de um sofrimento futuro daqueles que representam um risco à liberdade delas (VAZ; SÁ-CARVALHO; POMBO, 2005, p. 10). Na América Latina, isto é mais um reforço da tendência histórica do presidencialismo de se transformar em ditadura, pois dá mais controle às elites preocupadas, pois o presidente consegue absorver facilmente resistências do Legislativo. Em emblemática confissão do Plaza, ex-presidente do Equador, sobre tornar-se ditador diz ele que “seria preciso ter a alma de um Catão para resistir”.

Pela maior facilidade de avanço sobre direitos civis e as ações são justificadas pela necessidade de segurança, como os baculejos, inspeção pessoal por um agente de segurança diretamente no corpo do suspeito, forçosos majoritariamente em pessoas de pele mais escura. Genericamente, as soluções técnicas são frutos do cálculo de redução do ônus estatal em manutenção da ordem social. Do ponto de vista do Estado, é mais uma forma de vigilância e controle de cidadãos. Esta dissertação não é contra a vigilância em si, mas sim contra a tendência e o argumento inequívoco de que o Estado tudo pode em prol da segurança pública, ou seja, que pode atingir cidadãos sempre que haja a boa vontade da eficácia de seus meios,

argumento que pode justificar absolutamente qualquer intervenção estatal. São importantes estas reflexões, pois a mesma tendência existe hoje para a predileção de escutas telefônicas e de câmeras de vigilância em locais públicos, em que o julgamento se efetiva nos resultados. A executivização da política e a erosão dos poderes legislativos justificam quaisquer meios arbitrários do Estado. Uma moral de perigosa, pois justifica governos fascistas.

Como vimos no incentivo da técnica jurídica à submissão acrítica do homem, notamos a máxima de que “um direito que não é aplicado não é um direito” (ELLUL, 1968, p. 301). Logo, a consolidação de uma técnica jurídica fica mais centrada na eficácia do que na função de justiça, já que sempre haverá o argumento anterior à justiça de que é sempre necessário o aumento do controle estatal sobre a sociedade. Como consequência, a ideia de segurança substitui a finalidade de justiça (ELLUL, 1968, p. 301), valorizando-se a ordem e preocupando-se em prevenir o crime e evitar o sofrimento. E como vimos anteriormente, uma norma é mais eficaz na proporção que é menos desobedecida pelo povo. Dessa forma, a punição torna-se possível a quem possuir a possibilidade de tornar-se culpado e a violência policial contra as camadas mais pobres da população apresenta-se, logo, justificável pela contenção de riscos. A eficiência é um fato e a justiça social um mero slogan (ELLUL, 1968, p. 282). Vislumbrando uma solução, Ellul elucida que um Direito construído a partir de uma ideia de justiça é a única saída, mas que “esse conceito de justiça não pode surgir de dentro de uma racionalidade técnica” (ELLUL, 1968, p. 297) porque o jurista é apenas um racionalista subordinado aos resultados e ao padrão. Infelizmente, o autor não explica melhor o que seria na prática este conceito de justiça externo à racionalidade técnica. Afinal, uma noção de justiça bonita e bem escrita no papel da lei, mas que ninguém a cumpre – sem eficácia ou uma maioria a obedecendo – é desejável?

Não podemos afirmar sem especular que a tendência de Estado de Exceção advém de alguma vontade maquiavélica dos estatistas, dos empresários, do político, de partidos ou dos maiores detentores de capital. Independente da veracidade de tais conspirações, é a técnica quem se beneficia deste controle social e seu afastamento da ideia de justiça propaga um apoio a medidas drásticas de controle, em uma espécie de estado de exceção permanente aceita na cultura social, já que os cidadãos desejam a redução dos riscos para sua segurança. E a ausência de questionamentos dessas tendências impacta seriamente na tutela estatal da internet, onde qualquer comportamento técnico pode se autojustificar pelo medo do risco e do sofrimento de ações de terceiros e de cibercriminosos.

### 1.2.4 Características da Técnica

*Tudo que temos e somos necessita sempre ser o mais eficaz possível.*

Utilizaremos aqui a palavra técnica e não tecnologia porque tecnologia quer dizer estudo da técnica ou discurso sobre a técnica. De acordo com Ellul, a técnica contemporânea caracteriza-se pelo automatismo, autoacréscimo, unicidade, universalismo, autonomia e ambivalência. Além dessas seis características iniciais, temos também a racionalidade e a artificialidade, características que Ellul pouco se dedica por considerá-las evidentes. Racionalidade é a falta de espontaneidade e redução de fatos e fenômenos no esquema lógico, levando tudo a ser abreviado a uma equação; e Artificialidade é a forma articulada e generalizada como a técnica se impõe, por nossa necessidade completamente artificial de adquirir o mais tecnológico. Ademais, além destas oito características da técnica, adicionamos outras quatro que podem ser consequências das primeiras, mas são tão impactantes que merecem separada análise: alienadora, misantropa, sem finalidade e com efeitos imprevisíveis. São doze as características e como duas já foram explicadas, seguem as outras dez.

Ellul (1990, p. 18) entende ser o automatismo a impossibilidade de recusar a solução ou o método de maior racionalidade e eficácia, ou seja, é a automática escolha da forma mais eficaz – “a melhor escolha” – sempre. Assim sendo, a solução técnica mais eficaz se impõe a despeito os direitos mais subjetivos e menos palpáveis à técnica, como a liberdade e a privacidade do indivíduo. O método eficaz escolhido se converte no único método possível para se resolver um determinado problema. Assim, a eficácia é o fator do qual depende tudo, pois tudo que temos e somos necessita sempre ser o mais eficaz possível. Logo, automatismo significa que não existe uma verdadeira escolha entre várias técnicas, pois a mais eficaz se impõe independente de critérios religiosos, morais, filosóficos ou costumeiros. Por haver a aparência de outras possibilidades, parece existir uma liberdade de escolha. O ponto que Ellul traz é anterior à observação das possibilidades. Se vamos escolher todas as vezes sempre a mesma opção, a mais eficiente, para conduzir nossos atos, existe realmente uma liberdade de escolha? Assim, não há escolha entre dois métodos técnicos, pois o mais eficiente se impõe fatalmente porque seus resultados indiscutíveis:

Quando tudo tiver sido medido e calculado matematicamente de modo que o método decidido seja satisfatório do ponto de vista racional, e quando, do ponto de vista prático, o método for manifestamente o mais eficiente de todos os até então empregados ou aqueles em competição com ele, então o movimento técnico torna-se autodirigido. Eu chamo o processo de automatismo. [...] O ser humano não é mais, em nenhum sentido, o agente de escolha. [...] Ele pode decidir apenas a favor da

técnica que lhe dá a máxima eficiência. Mas isso não é escolha. Uma máquina pode efetuar a mesma operação. O homem ainda parece estar escolhendo quando abandona um determinado método que se mostrou excelente sob algum ponto de vista. Mas sua ação vem apenas do fato de ter analisado minuciosamente os resultados e determinado que, de outro ponto de vista, o método em questão é menos eficiente. [...] É sempre uma questão de aperfeiçoamento do método em si. [...] Dentro do círculo técnico, a escolha entre métodos, mecanismos, organizações e fórmulas é realizada automaticamente. O homem é despojado de sua faculdade de escolha e fica satisfeito. Ele aceita a situação quando fica do lado da técnica. [...] E quando tiver recebido plena satisfação e cumprido sua vocação, ficará sozinho no campo. A técnica revela-se assim ao mesmo tempo destruidora e criadora, e ninguém deseja ou pode dominá-la. (ELLUL, 1964, p. 79-85, tradução nossa).

Já o autocrescimento só pode ser observado quando a técnica produz a si própria, suscitando problemas de natureza técnica que exigem soluções que só a própria técnica resolve. Assim, o homem cada vez mais é impotente na detenção da progressão técnica porque os processos em cadeia o excluem cada vez mais, tornando-se futuramente um mero supervisor ou, para Ellul (1968, p. 93), um “dispositivo gravador de resultados”. Um exemplo é o exponencial uso da Inteligência Artificial no aprendizado de padrões comportamentais humanos a fim de gerar experiências personalizadas de tal maneira que nenhum outro ser humano poderia fazer igual. O autocrescimento significa que a técnica progride a despeito da intervenção humana. Assim, o ser humano vive em função da técnica que cria um ambiente propício para que outras apareçam. Por exemplo, os consumidores consomem o que a técnica pode produzir e não o que o produtor necessariamente deseja. Ellul cita o exemplo da descoberta do processo de combustão interna que levou às técnicas dos automóveis que levou a outras técnicas que criaram outras técnicas (ELLUL, 1964, p. 87). O progresso técnico é sempre diretamente proporcional ao nível econômico de um país, criando problemas técnicos que só podem ser resolvidos por outra técnica:

Atualmente, a técnica chegou a tal ponto de sua evolução que se transforma e progride quase sem intervenção decisiva do homem. [...] Todos trabalham nisso, e em todas as profissões ou ofícios todos procuram introduzir melhorias técnicas. O progresso técnico e o esforço humano comum dão no mesmo. [...] Há um crescimento automático (ou seja, um crescimento não calculado, desejado ou escolhido) de tudo o que diz respeito à técnica. [...] Dificilmente podemos concordar que o aumento mecânico está desacelerando. Estamos simplesmente em outra fase do progresso técnico: a fase de assimilação, organização e conquista das outras áreas. O ponto final a ser discutido ao discutir o autoaumento é essa técnica. em seu desenvolvimento, coloca principalmente problemas técnicos que, consequentemente, só podem ser resolvidos pela técnica. O nível técnico atual traz novos avanços, que por sua vez se somam às dificuldades e problemas técnicos existentes, que exigem ainda mais avanços. [...] Quanto mais fatores houver, mais facilmente eles se combinam e mais evidente é a necessidade urgente de cada avanço técnico. O avanço por si só se torna proporcionalmente maior e a expressão da autonomia humana proporcionalmente mais fraca. Os seres humanos são, de fato, sempre necessários. Mas literalmente qualquer um pode fazer o trabalho, desde que seja treinado para isso. Doravante, os homens poderão agir apenas em virtude de sua natureza mais comum e inferior, e não

em virtude do que possuem de superioridade e individualidade. (ELLUL, 1964, p. 85-92, tradução nossa).

Ellul observa que o fenômeno de conjunto das técnicas apresenta sempre a mesma lógica. A unicidade, também chamada de monismo, é a indistinção entre a técnica e o uso que dela se faz. A unicidade só é identificável por causa do princípio coincidente na organização de qualquer indústria e comércio e na manufatura de qualquer artefato e tecnologia: a necessidade de ser eficiente. Veremos durante a dissertação um estudo mais aprofundado sobre os produtos, mas adiantamos que o seu uso é inseparável do seu ser físico, não se pode diferenciar a técnica e o uso a que ela é destinada (ELLUL, 1964, p. 98). Quando se diz que o problema técnico não é culpa da técnica, mas sim do uso do homem, a técnica passa a não ser mais contestada nem julgada moralmente:

Existe uma noção atraente que aparentemente resolveria todos os problemas técnicos: que não é a técnica que está errada, mas o uso que os homens fazem dela. Consequentemente, se o uso for alterado, não haverá mais objeções à técnica. [...] Mas uma característica principal da técnica (que estudaremos longamente) é sua recusa em tolerar julgamentos morais. É absolutamente independente deles e os elimina de seu domínio. A técnica nunca observa a distinção entre uso moral e imoral. Tende, ao contrário, a criar uma moralidade técnica completamente independente. [...] Como já indiquei, vários usos sempre podem ser feitos da máquina, mas apenas um deles é o uso técnico. [...] Há apenas um método para seu uso, uma possibilidade. Dizer que tal meio técnico foi mal utilizado é dizer que nenhum uso técnico foi feito dele, que não foi feito para render o que poderia e deveria ter dado. Não há diferença alguma entre técnica e seu uso. O indivíduo se depara com uma escolha exclusiva, ou usar a técnica como deveria ser usada de acordo com as regras técnicas, ou não usá-la de forma alguma. É impossível usá-lo de outra forma que não seja de acordo com as regras técnicas. [...] Poderia citar inúmeros exemplos, mas os que dei bastam para mostrar que a técnica em si (e não o uso que dela se faz, ou as suas consequências desnecessárias) conduz a um certo sofrimento e a flagelos sociais que não pode ser completamente separada dele. Este é o seu próprio mecanismo. Quando o desvio específico para o ataque é encontrado, ele é usado. Seria tolice não usar os meios disponíveis. Mas nunca há tempo para estimar todas as repercussões. E, em todo caso, na maioria das vezes são imprevisíveis. Quanto mais entendermos a inter-relação de todas as disciplinas e a interação dos instrumentos, menos tempo haverá para medir esses efeitos com precisão. (ELLUL, 1964, p. 96-105, tradução nossa).

No universalismo, o processo de universalização da técnica apresenta dois momentos: o geográfico e o qualitativo (ELLUL, 1964, p. 116). Em escala global, os países que ainda não assimilaram alguma técnica almejam fazê-lo rapidamente. Afinal, a reivindicação dos países emergentes por desenvolvimento econômico é, na verdade, uma demanda de tecnificação. Note que o universalismo da técnica é assimilado hoje no conceito de globalização, uma palavra da moda com uma promessa de melhorias e progressos. Há malefícios e benefícios óbvios da globalização, mas a forma a qual a acatamos sem nem avaliar é um problema. Um exemplo de malefício é, em recorrentes crises do sistema financeiro internacional. Uma consequência imediata da assimilação técnica é a redução de culturas tradicionais a destroços recolhidos aos

museus, “como vestígios de épocas mortas” (ELLUL, 1968, p. 17). Afinal, estamos sempre cercados por inúmeras câmeras ou por *cookies* na rede quando se torna massa de manobra pelo fenômeno técnico, com massa sendo sinônimo daquele que não valoriza a si mesmo e se sente à vontade ao sentir-se idêntico aos demais (ORTEGA Y GASSET, 2001), o ser humano perde seu senso crítico e não compreende o outro, pois as opiniões se tornam divergentes e indiferentes. A regra natural é a antipatia pelo sofrimento alheio. Esta é a lógica universal:

Mesmo quando a população de um determinado país não está totalmente assimilada tecnicamente, ela é, no entanto, capaz de usar os instrumentos que a técnica põe em suas mãos. As pessoas desses países não precisam ser ocidentalizadas. A técnica, para ser utilizada, não requer um homem ‘civilizado’. A técnica, qualquer que seja a mão que a utilize, produz seu efeito mais ou menos totalmente na proporção da absorção mais ou menos total do indivíduo nela. [...] A invasão técnica não envolve a simples adição de novos valores aos antigos. Não põe vinho novo em odres velhos; não introduz novos conteúdos em formas antigas. As velhas garrafas estão todas sendo quebradas. As velhas civilizações desmoronam em contato com as novas. E o mesmo fenômeno aparece sob todas as formas culturais possíveis. [...] A técnica é um meio de apreensão da realidade, de atuação sobre o mundo, que permite desconsiderar todas as diferenças individuais, toda subjetividade. A técnica por si só é rigorosamente objetiva. Apaga todas as opiniões pessoais. Ele apaga todos os modos de expressão individuais e mesmo coletivos. Hoje o homem vive em virtude de sua participação em uma verdade tornada objetiva. A técnica não é mais do que uma ponte neutra entre a realidade e o homem abstrato. A técnica, além disso, cria um vínculo entre os homens. Todos os que seguem a mesma técnica estão unidos em uma fraternidade tácita e todos têm a mesma atitude perante a realidade. Não há necessidade de que conversem ou se entendam. (ELLUL, 1964, p. 116-131, tradução nossa).

A técnica desenvolve-se em obediência às suas próprias leis, não respeita qualquer oposição e parece ter força própria. A decorrência da autonomia é a técnica não tolerando ser julgada por ninguém, só por ela mesma. Ela é o valor supremo – de que a eficácia é o único fim da ação humana – e a instância última e irrecorrível, com julgamentos inapeláveis. Em casos de controvérsia como questões éticas e morais, a técnica se recusa a ser julgada e ainda forma uma nova moral. Condicionando e, assim, tudo que faz é permitido, lícito e justificado. É muito comum que pessoas, mesmo sem recompensa alguma, defenderem o uso de certa técnica para um bem maior sem conhecimento algum sobre o assunto. Esta tendência é culpa da sacralização da imagem e, também, da alienação provocada pela autonomia da técnica. O homem diante da técnica é reduzido a um animal técnico que não mais participa do desenvolvimento, ele apenas desencadeia o movimento e o objetivo da técnica é cada vez menos depender da ação humana, já que o homem é fonte de imperfeição, imprevisibilidade, tentado ao erro, um ser emocional que se cansa e se desencoraja. É por isso que o homem vem sendo substituído por máquina. Tanto que uma empresa que não é tecnificada ou mecanizada ou que não está no mundo real-virtual dificilmente sobreviverá, o artificial ganha espaço antes ocupado pelo homem natural.

Até no mundo das crianças de hoje, brincar é estar em contato com o mundo real-virtual. E assim, pelo medo da exclusão social, tornamo-nos dependentes:

As próprias necessidades internas da técnica são determinantes. A técnica tornou-se uma realidade em si mesma, autossuficiente, com suas leis especiais e suas próprias determinações. [...] Para ir um passo além, a autonomia técnica é aparente no que diz respeito à moral e aos valores espirituais. A técnica não tolera nenhum julgamento de fora e não aceita nenhuma limitação. [...] A moralidade julga os problemas morais; no que diz respeito a problemas técnicos; não tem nada a dizer. Somente critérios técnicos são relevantes. A técnica, ao julgar a si mesma, está claramente liberada desse principal obstáculo à ação humana. [...] Uma vez que se colocou além do bem e do mal, não precisa temer qualquer limitação. Por muito tempo se afirmou que a técnica era neutra. Hoje esta não é mais uma distinção útil. O poder e a autonomia da técnica estão tão bem assegurados que ela, por sua vez, se tornou a juíza da moral, a criadora de uma nova moral. Assim, desempenha também o papel de criador de uma nova civilização. Essa moral interna à técnica está assegurada de não sofrer com a técnica. Em todo o caso, no que diz respeito à moral tradicional, a técnica afirma-se como um poder independente. Somente o homem está sujeito, ao que parece, ao julgamento moral. Não vivemos mais naquela época primitiva em que as coisas eram boas ou más em si mesmas. A técnica em si não é nenhuma das duas coisas e pode, portanto, fazer o que quiser. É verdadeiramente autônomo. No entanto, a técnica não pode afirmar sua autonomia em relação às leis físicas ou biológicas. Em vez disso, os coloca para trabalhar; procura dominá-los. (ELLUL, 1964, p. 133-134, tradução nossa).

Além destas características, a técnica é ambivalente: ela libera (possibilidades), mas aliena (a tão somente uma real escolha de ação). Isto é, a ambivalência é a inseparabilidade dos efeitos nefastos dos positivos. Lembrando que não quer dizer sobre a possibilidade do mal uso de um objeto, porque, para ele, a técnica não é neutra. As análises mais rigorosas – construídas sobre dados estatísticos – são as mais perigosas porque são também elaboradas em função de ideologias, mas aparentam ser puramente científicas e com rigor antirretórico. Para Ellul (1990, p. 36), pela ambivalência, o desenvolvimento da técnica não é bom, nem mal e nem neutro, é uma mistura dos elementos indissociáveis positivos e negativos. Os bons resultados dependem do uso que fazemos do instrumental técnico, mas Ellul (1990, p. 34-35) cita que, com uma faca, pode-se descascar uma maçã ou matar um vizinho; chineses inventaram a pólvora para fogos de artifício, mas tinha outras potencialidades. E quanto mais a escolha de uso se torna impossível, mais é difícil escapar dos efeitos ambivalentes. Ellul traz quatro proposições que considera fatos sobre a ambivalência: todo progresso técnico tem seu preço, pois não é possível tirar os efeitos negativos do progresso positivo; em cada estágio, a técnica cria mais e mais problemas que só ela resolve; os efeitos negativos são inseparáveis dos positivos; e há uma série de efeitos negativos que desconhecemos – portanto, são imprevisíveis – antes de serem perpetuados (ELLUL, 1990, p. 39). Vejamos as seguintes alusões de Ellul:

A técnica pode ter efeitos bons e ruins. [...] Se queremos saber qual é o problema quando falamos de técnica, devemos começar por eliminar o argumento fútil sobre o seu uso. A ambivalência do progresso técnico é, infelizmente, mais complexa do que pode sugerir a visão simplista que acabamos de mencionar. Acreditar que tudo

depende do uso é achar que a técnica é neutra. [...] Não importa como é usado, tem em si uma série de consequências positivas e negativas. Isso não é apenas uma questão de intenção. Por um tempo, o uso pode orientar esta ou aquela técnica em uma direção puramente positiva, mas esta técnica tem em si potencialidades que são inevitavelmente exploradas. [...] As análises que parecem muito rigorosas, que se baseiam em estatísticas e que não fazem referência a estes problemas são as mais perigosas. Pois eles também são ideológicos, mas fingem ser puramente científicos e têm uma aparência de rigor que não se encontra em estudos mais retóricos, mas mais honestos. [...] O que quero dizer é que o desenvolvimento técnico não é bom, nem ruim, nem neutro. É uma mistura complexa de elementos positivos e negativos. Algumas são boas e outras são ruins, se quisermos usar termos morais. É impossível dissociá-los e assim conseguir uma técnica puramente boa. Além disso, bons resultados não dependem de forma alguma do uso que fazemos de equipamentos técnicos. Mas não basta enfatizar a ambivalência. Devemos analisá-lo, e o faremos com a ajuda de quatro proposições. Em primeiro lugar, todo progresso técnico tem seu preço. Em segundo lugar, em cada estágio ela levanta mais e maiores problemas do que resolve. Em terceiro lugar, seus efeitos nocivos são inseparáveis de seus efeitos benéficos. Quarto, tem um grande número de efeitos imprevistos. (ELLUL, 1990, p. 34-39, tradução nossa).

Ellul (1990, p. 38-39) diferencia ambivalência de ambiguidade, a primeira ambivalência implica há duas orientações precisas com valores opostos no mesmo objeto, já a ideia de ambiguidade é mais imprecisa. O que caracteriza a ambiguidade é o confuso e o indeterminado, e a técnica não é confusa nem indeterminada, mas perfeitamente certa:

Antes de proceder à análise da ambivalência, devo diferenciá-la de dois outros conceitos. A primeira é a da ambiguidade, que já enfatizei. Enquanto a ambivalência implica que um objeto tem duas orientações precisas e opostas, a ambiguidade é mais fluida. Ela carrega a noção do que é confuso, indeterminado, vago e equívoco. Mas a técnica não é fluida nem confusa, é precisa e nada equívoca. (ELLUL, 1990, 38-39, tradução nossa).

Um clássico discurso histórico foi e é a existência de um efeito perverso em certo evento ou artefato criado pelo homem. Como se existissem os efeitos normais e bons e os maus e que, no perverso caso, surpreendentemente, os maus perseveraram. Outra técnica humana de esquivar-se de responsabilidades. O ser humano – tão certo de suas virtudes, mas tão crítico das morais alheias – diz saber fazer um bom uso, o que significa absolutamente nada em termos de suprimir o lado maléfico de certa técnica. Ou seja, quanto mais a técnica aumenta, mais ampliam-se os perigos. Mas afinal, um objeto ou evento deverá ser ou acontecer de certa maneira justa e benéfica na opinião de quem, qual o ponto de referência para tal comparação? Como escapar deste histórico subjetivismo – do que é justo e bom para a sociedade – presente em ambas as extremidades, de tecnofilósofos e de técnicos-engenheiros, para justificar quais comportamentos e técnicas devemos adotar?

As seis últimas características descritas são originárias da doutrina de Ellul. Apesar de ele apenas mencionar as próximas quatro em algum ponto, elas merecem destaque na classificação de características pois são marcantes, especialmente quanto ao objeto dessa

dissertação: a internet. Quanto à alienação, a técnica deixa de ser instrumento de racionalização para ser instrumento de dominação das atividades humanas. Assim, o homem participa da técnica, mas como se ele fosse uma coisa, e a técnica faz questão de alienar o homem de todas formas: no trabalho, pois a especialização o leva a desconhecer todo o resto; em sua mentalidade, tratando todas suas morais e espiritualidades como descartáveis; e na sua imagem, o obrigado a transparecer algo que verdadeiramente não é. Aliena e controla o ser humano em todas suas formas para transformá-lo o máximo possível em inanimado e inumano, em um técnico. A técnica torna o homem aparentemente livre para buscar o que bem quiser e sua alienação o faz buscar coisas que também aparentemente lhe trariam felicidade, mas ele foi programado e induzido a buscar tais coisas. O que ele quer foi mudado pela técnica, ele deseja o que a técnica, com a da propaganda ou autopromoção, deixa a disposição. Se a técnica controla o que o ser humano quer, controla o que existe para o ser humano querer, pré-estipula a única escolha – a mais eficaz – e as possibilidades, logo, ela impõe. E a internet é uma criação humana que nem o homem realmente compreende. A ideia contemporânea de alienação surge com Karl Marx (1867) como um fenômeno ideológico ocasionado pelas condições de trabalho. Apesar da expressão ter sido banalizada nos tempos modernos, como anticapitalista, o termo aqui posto não tem a ver com Economia, mas sim com desumanas padronizações de comportamento. A busca por eficiência e produtividade aliena a ética e a responsabilidade humana. Até o sexo passou a ser um alienador objeto de consumo buscado incessantemente e, muitas vezes, não por um estímulo de natureza biológica de dentro do seu íntimo, mas provocado – de fora para dentro – por um apelo artificial ao sexy e à luxúria.

Misantropia (do grego μῖσος – ódio – e ἄνθρωπος – ser humano) é a aversão ao ser humano e à natureza humana no geral, englobando uma posição de desconfiança e antipatia com outras pessoas. Misanthropo é, portanto, alguém que odeia a humanidade de uma forma generalizada. Apesar de alguns humanos serem assim, interessa-nos que tal característica está sempre presente na técnica, que afasta do humano sua humanidade e individualidade. A alienação, como de seu tempo e de seu trabalho, traz anestésias que evitam aborrecimentos, conflitos e cansaços oriundos de decisões, talvez levando até a uma espécie de felicidade ou paz. O que traduz, todavia, numa diminuição da personalidade humana. A misantropia da técnica é a aversão que ela tem do homem falível, sentimental e julgador. O homem que a técnica “busca” é uma máquina, um técnico, um ser inanimado e, portanto, não é um ser humano, é o homem de massas. Essa massificação psicológica procura a felicidade do homem no sentimento coletivo juntamente com sua utilização. O homem-máquina ideal não é homem nem humano; ser humano somente quando permitido é, no máximo, um ser-humano-quando-

dá. Quando o indivíduo não reconhece sua individualidade, perde seus valores ideológicos e morais e ganha os novos valores de racionalidade técnica.

A penúltima característica que identificamos é a falta de finalidade da técnica. Vejamos que a realidade da técnica se impõe independente da decisão humana, isto é, a noção de finalidade é estranha à técnica uma vez que esta evolui causalmente. Observemos que a alienação ou a misantropia são meios ou consequências da técnica, mas não são a finalidade. A técnica não “quer” acabar com o lado humano do homem, ela o esgota porque é necessário. A técnica não “quer” que o ser humano seja eficiente, ela automaticamente impõe que ele o seja. Ter uma intenção finalística e se utilizar de certo meio são coisas distintas. No fenômeno da técnica, todos fatos ou objetos que citamos até agora são meios, não um fim em si. Mas meios para que? Não há como supor epistemologicamente. Técnica não é uma inteligência artificial avançada que controla todas máquinas e tecnologias e que devemos combatê-la. Ela não tem consciência, é tão somente o constante querer ser eficaz pela padronização através de conhecimento científico. Seria como perguntar qual o fim da avalanche de neve. Sabemos o porquê que acontece e como (através de gravidade e montantes de gelo), mas ela não tem uma finalidade (de deslocamento vertical da água solidificada) e sim apenas consequências. A chuva não ocorre para atender a um fim, como o de irrigar as plantas. Ela pode ser consequência de eventos químico-biológicos e ter suas próprias consequências, mas não tem o propósito para isso. Ela é um evento inanimado e, portanto, sem finalidade. A técnica é como qualquer evento ou objeto natural porque são criados por algo, mas não têm uma finalidade específica. Se alguém a atribui alguma finalidade, isto é um posterior uso humano. E se são causas para outros eventos, não são finalísticas para estes, mas sim meros elementos interativos com um todo. Resta nos perguntar qual é a explicação dos cientistas e técnicos neste progresso humano. Muitas vezes, parece ser a felicidade da humanidade. Os defensores do *status quo* justificam que se tem pelo menos uma pessoa realizando certa ação ou pesquisa, há certo interesse social – mínimo, quando se trata de um só humano – e que, portanto, há justificativa de pelo menos ser para a felicidade daquele. Para Ellul, eventuais normas jurídicas, éticas ou morais não serão barreiras suficientes para frear seu desenvolvimento ambivalente. E se não há diferença entre a técnica e seu uso porque o único uso correto é o uso técnico, não há como orientar a técnica de acordo com normas ou padrões morais que hipoteticamente tornariam justo o seu emprego. Em outras palavras, sua evolução puramente causal, do progresso técnico e científico, nos conduz cegamente ao futuro.

A imprevisibilidade é a última das características gerais da técnica. Vejamos que todo progresso técnico apresenta três tipos de efeito: os desejados, os previsíveis e os imprevisíveis

(logo, indesejados). O conhecimento científico padroniza comportamentos e experiências a fim de se estabelecer métodos que gerem resultados previsíveis, precisos e claros. O efeito desejado é mais fácil de se notar. Enfrenta-se a necessidade de locomover-se o mais rápido possível de um ponto a outro à 2 mil quilômetros de distância. Logo, criam-se um conjunto de técnicas para resolver o problema. Esses são os efeitos desejados, com procedimentos técnicos de aplicação que esperam um certo número de resultados e, geralmente, os obtêm. A técnica é bastante segura que dará os efeitos esperados e, mesmo se fracassasse, o progresso técnico eliminaria as incertezas. Os segundos efeitos são os não procurados, porém previsíveis. Por exemplo, ingerir certos remédios podem levar a acidentes graves (como neurolépticos e antiespasmódicos), mas justificam-se porque seu risco é inferior aos benefícios esperados. É necessário então fazer uma avaliação do risco conhecido e do benefício previsível. E a terceira categoria de efeitos é a total imprevisibilidade, os que muito preocupam Ellul (1990). Os efeitos imprevisíveis esperados se originam na nossa incapacidade de prever com exatidão um fenômeno, já os imprevisíveis e inesperados são aqueles sem qualquer previsão e que permanecem hipotéticos, pois geralmente são eventos que a humanidade ainda não experimentou para aprendê-los e, logo, prevê-los.

O progresso técnico não é medido por consequências, isto é, não há limites morais, religiosos ou filosóficos para esse desenvolvimento. É o meio (racional) que justifica (qualquer que seja) o fim porque não há como agir melhor do que racional e tecnicamente. Portanto, qualquer que seja o grau de nocividade da consequência de um ato ou artefato técnico, ele será interpretado como inevitável e encontrarão motivos para crer que teria sido pior sem o mesmo. Desconhecer causas e efeitos de fenômenos é ser fraco e imprevisível e a técnica e o homem técnico jamais reconheceriam suas ignorâncias. É por isso, por exemplo, que o uso intencional de queimadas em plantações, o uso de transgênicos, energias nucleares e pesticidas são justificáveis. Nunca se saberá certamente todos os efeitos especialmente porque a sociedade técnica muito se preocupa com sua própria especialização, não levando em conta os efeitos produzidos na sociedade e nos outros, inclusive em nível inconsciente.

### 1.3 TECNOLOGIA: CONCEITUAÇÃO E INFLUÊNCIAS

*A tecnologia busca mudar o mundo.*

Desde o início da História do homem, ao talhar o sílex de seus instrumentos de guerra, o homem manifesta arte já na escolha da forma dessas armas e de seus ornamentos. Essa arte

adquire consciência nos tempos modernos ao visar uma finalidade utilitária (SILVEIRA, 2014). Ao fabricar seus primeiros utensílios artificiais o homem começa a ser dominado pela técnica. Quando ele cria sua primeira proteção de pele animal – roupa primitiva – ou a primeira pedra lascada e galho pontiagudo para caça ou pedaço de pau para combate, ele acaba sendo dominado no sentido de que, sem os mesmos, ele voltaria a ser comum e inferior àqueles que os detém. Este homem primitivo pode não ter percebido pronta e conscientemente, mas observando a experiência alheia e notando que caçava melhor, obtinha melhores comidas, tinha menos doenças com vestimentas e melhor sucesso em combate com estes instrumentos, não pôde mais se dissociar deles. Se não os tivesse consigo, era como se estivesse despido, vulnerável. A técnica deu e dá, desde o homem mais primitivo, proteção contra o risco externo e conforto em seu mundo interno. Numa visão darwiniana, a instrumentalização de artefatos pelo primeiro homem – o *orrorin tugenensis* – o fez adaptar melhor que seu antecessor, o *sahelanthropus tchadensis*.

É desta maneira que o ser-no-mundo lida com as coisas ao seu redor, ou seja, que toma os utensílios e os usa (HEIDEGGER, 1996). Para melhor aprofundarmos na tecnologia, devemos elucidar o que é este utensílio e a sua essência. Pode-se dizer que a tecnologia tem duas dimensões: a instrumentalidade, de interferência proposital do ambiente e de suas vidas; e a produtividade; do esforço humano na criação de coisas novas, controladas e inteligentes (FRANSSEN; LOKHORST; VAN DE POEL, 2018). Assim, a tecnologia é algo artificial que tem um fim. Às vezes a tecnologia tem uma finalidade mais direta, outras vezes tem a finalidade de criar algo que deve criar outra coisa ou tarefa finalmente. Vejamos que é muito difícil notar os impactos práticos que certo artefato e algo novo têm sobre a vida, cultura e sociedade humana. É quase imperceptível a alteração sistêmica da realidade resultante de cada artefato produzido. As alterações específicas são mais claras e notáveis; mas as sistêmicas, não tanto.

A tecnologia é uma tentativa contínua de aproximar o mundo da maneira que se deseja. Enquanto a ciência busca entender o mundo como ele é, a tecnologia busca mudar o mundo. Por um lado, de quem são os desejos modificadores da aparência do mundo pela tecnologia? Ao contrário dos cientistas, motivados em entender o mundo, os engenheiros são vistos como serventes do público e meros instrumentos do mercado (FRANSSEN; LOKHORST; VAN DE POEL, 2018). Emmanuel G. Mesthene (1970) define tecnologia como a organização do conhecimento para alcançar objetivos práticos. Já Thomas P. Hughes (2005, p. 3, tradução nossa) oferece duas definições de tecnologia: “um processo de criatividade que envolve engenhosidade humana” e o “esforço para organizar o mundo para a solução de problemas, de modo que bens e serviços possam ser inventados, desenvolvidos, produzidos e usados”

(HUGHES, 2004, p. 6, tradução nossa). E Joel Mokyr (1992, p. 6, tradução nossa) define progresso tecnológico como “qualquer alteração na aplicação de informações ao processo de produção de forma a aumentar a eficiência, resultando na produção de uma determinada produção com menos recursos (ou seja, custos mais baixos) ou a produção de produtos melhores ou novos”. Vejamos uma valorosa ponderação de David M. Kaplan sobre o tema:

As tecnologias são melhor vistas como sistemas que combinam técnicas e atividades com implementos e artefatos, dentro de um contexto social da organização em que as tecnologias são desenvolvidas, empregadas e administradas. Eles alteram os padrões de atividade e instituições humanas, criando mundos que moldam nossa cultura e nosso ambiente. Se a tecnologia consiste não apenas em ferramentas, implementos e artefatos, mas também em redes inteiras de relações sociais que estruturam, limitam e possibilitam a vida social, então podemos dizer que existe um círculo entre a humanidade e a tecnologia, cada uma moldando e afetando a outra. As tecnologias são criadas para refletir e estender interesses, atividades e arranjos sociais humanos, que são, por sua vez, condicionados, estruturados e transformados por sistemas tecnológicos. (KAPLAN, 2003, tradução nossa).

O que impulsiona o processo de inovação é importante para quem está preocupado com seu papel na sociedade, a fim de ser mais que mero instrumento social e do mercado e de se entender como humano cujas ações têm consequência para todos. Assim, a tecnologia ou engenharia estão relacionados à criação de artefatos pelo processo estruturado de design. No início deste processo, estão as necessidades ou desejos do cliente que são traduzidos na tarefa de design que um engenheiro deve cumprir. Na segunda etapa, os requisitos funcionais são retratados em termos mais específicos e práticos que serão os parâmetros de design dos requisitos funcionais (FRANSSEN; LOKHORST; VAN DE POEL, 2018). A complexidade de um dispositivo, logicamente, afeta seus requisitos funcionais, como a dificuldade em mantê-lo, a facilidade de manutenção, o ciclo de vida e os custos de reparo. Na engenharia da computação, uma das áreas da presente dissertação, não pode um desenvolvedor criar um software – como um site ou rede social – e esperar nunca mais melhorá-lo, especialmente numa sociedade cujos desejos são tão dinâmicos. Muitos empecilhos de um artefato são más definições ou “perversos problemas”, sem clara solução. Seria o artefato em si o problema, o mundo que o interpreta, a plataforma a qual ele está inserido ou o uso que fazem dele? Observa-se que muitas técnicas de resolução de problemas ou softwares disponibilizados por empresas são tratados como únicas soluções a serem tomadas, pois não as pessoas não buscam outras melhorias para o mesmo problema. Esses problemas perversos são geralmente obstáculos sociais que seriam melhor atendidos por alguma forma de ação social, com povos modificando seus comportamentos, de modo que o problema fosse mitigado até desaparecer. Contudo, o repertório de formas comprovadamente eficazes de ação social é escasso. Como dissemos no subcapítulo “História

do Homem Técnico”, o apelo pela consciência coletiva historicamente não rendeu seus bons frutos. Como possível solução, as correções técnicas poderiam ser superadas pela inclusão das ciências sociais no desenvolvimento e aplicação do conhecimento científico; para outros, estes espectros deveriam ser mantidos à maior distância possível um do outro, como ainda veremos.

Outro exemplo de problemática que assola a falta de controle sobre a tecnologia é o malefício de um *cookie* ser compartilhado irresponsavelmente entre empresas ser muito pequeno em comparação com o malefício do dano moral e do constrangimento por falhas destes provedores. A moralidade é um conceito muito subjetivo a qual a descrição de uma tecnologia não poderia ser alterada por causa do mesmo; não há força natural da engenharia, da computação neste caso, que buscaria modificá-lo e conseguiria tão somente por isto. Neste sentido, há a importância de modificação artificial destes artefatos a fim de defender alguma moral humana, só ocorrendo se esse objeto for tratado como normativo e influenciador de morais. As ideias sobre o que a ciência do design é e deve ser estão relacionadas aos problemas do raciocínio moral de meios-fins (FRANSSEN; LOKHORST; VAN DE POEL, 2018). E aqui desdobra nosso próximo subcapítulo.

### 1.3.1 Ética na Tecnologia

*A ética na tecnologia se tende à moralização da tecnologia.*

No século XX, começou o desenvolvimento da ética da tecnologia como uma subdisciplina independente da filosofia. Desde a antiguidade, observou-se que novos recursos podem ser mal utilizados ou levar à arrogância humana. Muitas vezes, no entanto, essas consequências indesejáveis são atribuídas ao uso de usuários e não à própria tecnologia ou a seus desenvolvedores. Como já visto, essa é a visão instrumental da tecnologia, resultando na chamada tese da neutralidade do artefato, muito comum em discursos sobre certos problemas na internet como a noção de que um provedor nunca deve se responsabilizar ou fazer nada a respeito sem a ordem judicial quando um usuário utiliza sua plataforma para algum mal, como no caso de retratação de discursos de ódio em redes sociais. Assim, a tese da neutralidade sustenta que a tecnologia é um instrumento neutro que pode ser usado de maneira boa ou ruim por seus usuários. Essa tese da neutralidade recebeu críticas de Heidegger (1977, p. 3-35) e Ellul (1968).

Devemos notar os tipos de relação do homem e da tecnologia com o mundo. A relação de incorporação é o: (Humano  $\rightarrow$  tecnologia)  $\rightarrow$  Mundo. Já a relação hermenêutica é o: Humano  $\rightarrow$  (tecnologia  $\rightarrow$  mundo). A relação de alteridade é o: Humano  $\rightarrow$  Tecnologia (mundo). E, por fim, a relação de fundo é o: Humano (tecnologia / mundo) (IHDE, 1983). Na primeira relação, as tecnologias formam uma unidade com o ser humano direcionada ao mundo, como falar com outras pessoas através de apps de videochamadas, em vez de falar com o telefone em si; olhamos através de um telescópio, não para ele. A segunda são as relações nas quais os seres humanos leem como as tecnologias interpretam o mundo, sendo direcionados pela máquina, como um equipamento de raio X que fotografa partes internas do corpo ou o sinal sonoro de uma chamada telefônica. Já na relação de alteridade, os seres humanos interagem com as tecnologias, com o mundo no fundo dessa interação, por exemplo obter dinheiro em um caixa eletrônico ou operar uma máquina. E, por fim, nas relações de fundo, as tecnologias são o contexto das experiências e ações humanas, como números dos radares eletrônicos e os sons de notificação dos celulares, ou seja, as tecnologias são um contexto para a existência humana em vez de serem experimentadas (IHDE, 1990). Percebe-se uma tendência cada vez maior de tecnologias desta última relação porque o ser humano quer mimetizar ao máximo as relações, uma vez, humanas.

Uma outra observação é o dilema de Collingridge. Este dilema trata do fato de que, quando uma tecnologia ainda está em um estágio inicial de elaboração, ainda é possível influenciar a direção de seu desenvolvimento, mas sem saber como afetará a sociedade. No entanto, quando a tecnologia é incorporada socialmente, sabemos suas implicações sociais iniciais, mas é muito mais difícil influenciar seu desenvolvimento. O dilema é um dos maiores desafios para o design de inovações responsáveis e é também uma preocupação de Ellul, visto que dificilmente podemos frear um desenvolvimento técnico ou tecnológico. Vislumbramos este problema na internet, quando só depois de se inserir um aplicativo no mercado, nota-se suas más consequências, como o app Lulu, em que seus usuários, a maioria mulheres, avaliavam perfis de homens, muitas vezes sem permissão. Por usar dados de usuários sem autorização, por meio do Facebook, o app foi obrigado a sair do ar no início de 2014. E a responsabilização sobre estas más consequências é uma meta deste trabalho pois devemos buscar uma reparação satisfatória das falhas informáticas. Todavia, estratégias que buscam escapar deste dilema através de experimentos responsáveis não podem prescindir todos quadros hipotéticos. Assim, jaz o dilema de tornar a antecipação muito especulativa (o risco da mudança tecnomoral) ou desistir demais da antecipação (o risco da experimentação sociotécnica), consequência dos valores usados para avaliar tecnologias serem co-constituídos por elas. Ellul diria ser causa do

autocrescimento técnico. Uma melhor compreensão de valor humano pode contribuir substancialmente para o design e uso de tecnologias mais responsáveis. Ou seja, a ética na tecnologia se tende à moralização da tecnologia.

Como projetar artefato é o tema que mais nos interessa, devemos compreendê-lo. Os artefatos são os objetos feitos pelo homem e os mais relevantes são artificialmente criados para servir a um propósito técnico. Ou seja, não se inclui aqui os subprodutos e resíduos (resultados de um ato sem intenção específica) e obras de arte (de intenção somente na criação e não na sua utilidade). Seja produto final ou componente, um artefato tem a função de servir. Mas até o momento, não existe uma consolidada noção que cubra tanto a noção de função artefato baseada na intencionalidade quanto a noção não-intencional (FRANSSEN; LOKHORST; VAN DE POEL, 2018). Como um artefato pode ser usado para uma finalidade diferente da pretendida pelo designer, deduz-se que artefatos possam ter várias funções ou impõe-se uma hierarquia entre todas. As últimas intenções seriam chamadas de acidentais e este uso acidental é a fonte dos principais problemas na internet e que o Direito Digital tenta resolver. Afinal, não se pode criar um artefato projetando com a intenção de que seja usado para um único fim específico. Franssen, Lokhorst e Van de Poel (2018) trazem como exemplos os tipos básicos de tecnologia da “faca” e do seu tipo funcional de “cortador”, em que uma faca é definida pela intenção de corte e por algum princípio operacional conhecido do design (como o tamanho para distingui-la de um facão ou a utilidade para distingui-la de uma espada); então, uma faca é uma forma específica de cortador, mas um cortador se refere ao tipo funcional e conflitante entre uso e design porque vários artefatos podem cortar:

Intimamente relacionado a essa questão em que medida o uso e o design determinam a função de um artefato está o problema de caracterizar os tipos de artefatos. Pode parecer que usamos funções para classificar artefatos: um objeto é uma faca porque tem a função de cortar, ou mais precisamente, de nos permitir cortar. Em uma inspeção mais detalhada, no entanto, a ligação entre a função e o tipo de associação parece muito menos direta. Os tipos básicos em tecnologia são, por exemplo, ‘faca’, ‘avião’ e ‘pistão’. Os membros desse tipo foram projetados para serem usados para cortar algo, transportar algo pelo ar e gerar movimento mecânico por expansão termodinâmica. No entanto, não se pode criar um determinado tipo de artefato apenas projetando algo com a intenção de ser usado para algum propósito específico: um membro do tipo assim criado deve realmente ser útil para esse propósito. Apesar de inúmeras tentativas e reivindicações de design, a máquina de movimento perpétuo não é um tipo de artefato. Um tipo como ‘faca’ é definido, portanto, não apenas pelas intenções dos projetistas de seus membros de que cada um seja útil para cortar, mas também por um princípio operacional compartilhado conhecido por esses projetistas e no qual eles basearam seu projeto. [...] Como tipos de tipos nos quais os artefatos podem ser agrupados, uma distinção deve, portanto, ser feita entre um tipo como ‘faca’ e um tipo correspondente, mas diferente, ‘cortador’. Uma ‘faca’ indica uma maneira particular de fazer um ‘cortador’. Pode-se também cortar, porém, com fio ou linha, maçarico de solda, jato d’água e, sem dúvida, por outros meios que ainda não foram pensados. Um ‘cortador’ se referiria a um tipo verdadeiramente funcional. Como tal, está sujeito ao conflito entre uso e design: pode-se entender por ‘cortador’ qualquer coisa que possa ser usada para cortar ou qualquer coisa que tenha sido

projetada para ser usada para cortar, pela aplicação de qualquer princípio operacional, atualmente conhecido ou desconhecido. (FRANSSEN; LOKHORST; VAN DE POEL, 2018, tradução nossa)

E por que esta discussão é importante para nós? Pois na internet há tantos artefatos virtuais com tantas utilidades distintas que os tipos funcionais – e, logo, também os acidentais – são variáveis com seus específicos atributos. E, para a filosofia da tecnologia, temos de encontrar algum tipo de responsabilidade para além do artefato em si. Por isso, produzir normas ou decisões jurisprudenciais para, por exemplo, todos tipos de redes sociais pode ser um erro, pois ignora as características específicas de cada uma, como aquelas que utilizam algum processo de editoração. Até dentro de uma rede social, podem haver múltiplos artefatos, como os *cookies*, que trabalham de formas diferentes e devem ser avaliados também separadamente. Por exemplo, o cookie que capta a busca no Google e na barra de tarefas do próprio site serve para oferecer propagandas mais direcionadas; os cookies que captam pesquisas de usuários buscam sugerir “amigos” ou até parceiros amorosos com maior precisão; os cookies que captam pesquisas por livros, autores ou esportes e times buscam assimilar estes gostos pessoais para sugerir novos gostos que o usuário pode aproveitar.

Franssen, Lokhorst e van de Poel (2018) trazem quatro problemáticas da Ética da Tecnologia. O primeiro tema da ética da tecnologia que trazem é saber se a tecnologia é carregada de valor (agência moral) ou se ela é neutra. Como vimos, alguns autores sustentam que a tecnologia é um meio neutro para um fim e, portanto, pode ser usada de maneira boa ou ruim. Essa visão é plausível na medida em que a tecnologia é considerada apenas uma estrutura física simples. A maioria dos filósofos da tecnologia, no entanto, concorda que a conexão conceitual entre artefatos tecnológicos, funções e objetivos dificulta a noção de tecnologia neutra em valor. Este debate sobre agência moral e tecnologia é discutido academicamente no design de inteligências artificiais, pois talvez seja impossível projetar agentes éticos completo e talvez seja imoral fazê-los. Afinal, se a agência moral da técnica limita nosso livre arbítrio, temos realmente escolha perante a gloriosa técnica?

O segundo tema que trazem os autores é a responsabilidade, instituto que o Direito se preocupa mais. Antigamente, não havia uma responsabilização dos engenheiros por suas criações, que “as apreciam sem conseguir dirigi-las” (ELLUL, 1968). Geralmente, na responsabilidade dos engenheiros, há a moral finalística da técnica em que tudo é realizável porque serve à felicidade humana. É difícil reconhecer uma responsabilidade individual na engenharia da computação já que há outros fatores, como o mal uso pelo usuário, restrições de mercado e a impossibilidade de prever certa consequência negativa. Outro problema é o da

indução, afinal, ao procurar um padrão moral que explica certo fenômeno e que se aplica a todos os casos isolados análogos, pode-se não englobar todos os fatores que influenciam este fenômeno, levando-se a um grave erro. Por fim, outra dificuldade de atribuir responsabilidade individual encontrada pelos supracitados autores é o frequente Problema de Muitas Mãos (PMH) em ambientes coletivos (FRANSSEN; LOKHORST; VAN DE POEL, 2018). Por exemplo, no emblemático e caricaturesco depoimento do CEO do Facebook Mark Zuckerberg no Congresso Americano, todas as vezes que os congressistas perguntavam, ele respondia que perguntaria a seus engenheiros se era possível; e quando apontavam um erro ou problema, respondia que não tinha domínio sobre aquela situação provocada pela sua rede social, mesmo tendo criado a plataforma e sendo o CEO da companhia. Todas soluções para este problema basicamente pairam em conhecer o máximo de fatores possíveis e compartilhar responsabilidades. No Direito, porém, estas soluções para o Problema de Muitas Mãos não têm um prático proveito. A internet cria diversos problemas que demandam bastante coordenação conjunta (como a identificação e captura de cibercriminosos), o que dificilmente ocorre, sendo este outro empecilho na busca de responsabilização e reparação dos danos.

O terceiro tema são os riscos tecnológicos, pois como já vimos no subcapítulo “Risco e Sofrimento no Estado”, eles levantam questões éticas e teóricas. O risco é geralmente definido como “produto da probabilidade de um evento e de seu efeito indesejável, quanto maior o risco, maior a probabilidade do evento indesejável” (FRANSSEN; LOKHORST; VAN DE POEL, 2018, tradução nossa). Uma redução de riscos pode ser inviabilizada porque não existem tecnologias absolutamente seguras ou a melhora demandaria uma grande despesa ou pode não ser desejável do ponto de vista moral. Como reduzir o risco do produto através de uma deslocação de recursos – para a área de pesquisa da empresa – que retiraria mais ainda a folha salarial de empregados. A redução de riscos geralmente tem um custo, bem vimos esta indissociabilidade do lado positivo (a redução de riscos) com o negativo (o custo). Afinal, produtos mais seguros podem ser mais difíceis de usar, mais caros ou menos sustentáveis e é o mercado que responde o que é seguro o suficiente e o que torna um risco aceitável. Outro problema são os dois tipos de erros possíveis: estabelecer um risco quando não existe ou concluir erroneamente que não há risco enquanto existe. A ciência, como ente econômico do mercado, tradicionalmente evita o primeiro porque sua negação gera maior liberdade de criação, mas para vários autores como Ellul, o segundo erro é o mais perigoso. Afinal, uma falta dessa avaliação aumenta certos riscos tecnológicos que podem afetar amplamente os usuários, como um governo recolher dados sensíveis da população para fins informativos e não se preocupar nem considerar o risco de falhas de segurança da guarda dos dados de seus cidadãos. Vejamos

que diferentes critérios de decisão podem ser aplicados na análise de um custo-benefício. Esta ponderação, assim como qualquer outra em todas áreas incluindo a de Alexy (2009) com sua ponderação, somente explica o significado de custo-benefício e quase nunca incita concretos efeitos. Um clássico no Direito Digital são as constantes recusas da empresa Apple em criar um meio para que o Estado americano possa desbloquear iPhones apreendidos a fim de colher provas contra criminosos. Para a empresa, gerar-se-ia uma brecha de segurança com risco muito grande para seus dispositivos; custo tão grande que compensa, na visão da empresa, as sanções financeiras dos EUA. Outra abordagem é basear a aceitação generalizada e consentida dos riscos pelas pessoas que os sofrem. E, mesmo assim, o consentimento informado na internet, como veremos no subcapítulo “Consentimento Quase-Tácito”, na maioria das vezes passa a ser tácito e rapidamente “aceito” sem grandes consolidações de direitos. Resta sempre a questão de que os problemas podem sempre afetar a sociedade como um todo indiretamente, na economia ou na *psique* humana. Para outros autores, se muitas vezes nos falta conhecimento para avaliar os riscos de uma nova tecnologia (como a probabilidade de erro e as possíveis consequências negativas), então não há necessidade de considerá-los previamente. Logo, a abstenção inicial seria a melhor solução. Muito parecido com a posição dos já citados defensores do *status quo*.

E o quarto e último tema que trazem os autores é a moda do *by design* da tecnologia, como a tendência do *privacy by design*, em que durante a fase inicial de criação de tecnologias suas consequências sociais ainda são mais maleáveis e evitáveis se ruins. Ao tentar integrar valores ao design, temos o problema de conflito de valores. Por exemplo, o carro mais seguro não é, devido ao seu peso, provavelmente o mais sustentável (FRANSSEN; LOKHORST; VAN DE POEL, 2018). São muitas as interpretações sobre dados para julgar como bom um certo artefato no final das contas. Mas sejamos claros, quando engenheiros lidam com esses conflitos e fazem a análise de custo-benefício com múltiplos critérios, tratar-se-á sempre de critérios subjetivos a cada técnico julgador. Portanto, é crucial que o Direito estabeleça parâmetros claros e objetivos na formação e criação de tecnologias se quiser evitar tais consequências sociais.

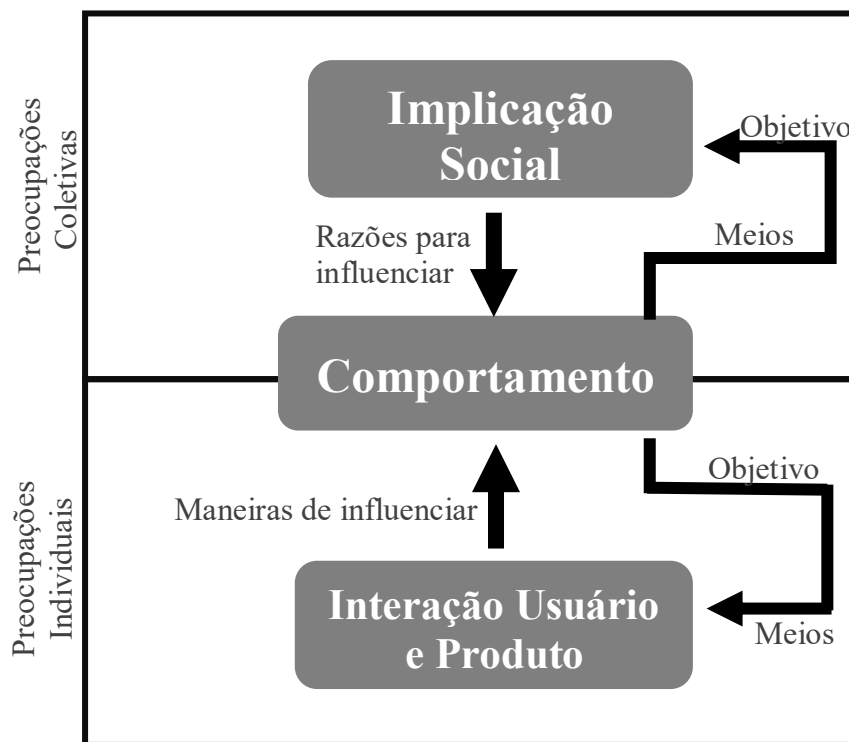
### 1.3.2 Influências de Produtos nos Indivíduos

*O design é uma tentativa de alterar o comportamento.*

Não é novidade que produtos têm implicações para o ser humano. Filósofos e sociólogos recorrentemente observam efeitos não intencionais de produtos sobre o humano. Verbeek

(2005) usa o exemplo do micro-ondas para mostrar que o design também pode não intencionalmente influenciar os padrões de comportamento, já que ele pode ter sido um dos fatores de diminuição do tempo de janta em família, em comparação com antes. Este exemplo mostra que os produtos podem mediar certo comportamento sem determiná-lo. Afinal, as famílias podem ainda manter seus antigos padrões alimentares. Verbeek (2005) explica que um produto não é um intermediário neutro, mas um mediador ativo do usuário e de seu ambiente. Também é perceptível na internet, com *apps* modificando nosso cotidiano. Ou seja, existem diferentes maneiras pelas quais o design afeta comportamentos e, portanto, têm implicações para a sociedade, tanto intencionais quanto não intencionais. Assim sendo, o design é uma tentativa de alterar o comportamento.

Quadro 01 - Como o comportamento forma um estágio intermediário entre implicações sociais e a interação usuário-produto e, portanto, respectivamente, entre preocupações coletivas e individuais.



(Fonte: TROMP; HEKKERT; VERBEEK, 2011, tradução nossa)

Vejamos, pelo Quadro 01, as interações do usuário e do produto a fim de alterar comportamentos por alguma implicação social. Para melhor exemplificar o quadro acima, Tromp, Hekkert e Verbeek (2011) trazem o tamanho de um prato. Pessoas que usam um prato pequeno servem menos comida e, portanto, comem menos que as pessoas que usam um prato grande. Ou seja, este produto muda a forma de servir alimentos e influencia o comportamento

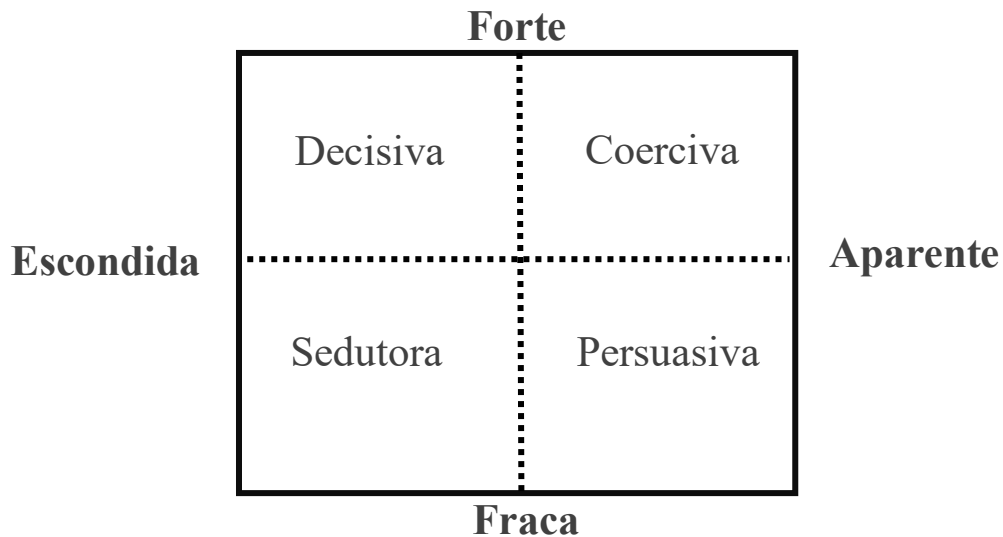
alimentar. Para um engenheiro-designer preocupado com obesidade, mudar o comportamento alimentar das pessoas ao alterar a quantidade de comida servida é uma maneira de fazê-lo e projetar atrativos alimentos saudáveis pode ser uma outra maneira. Pessoas interagindo com o pequeno prato servem menos porque é uma resposta automática ou podem fazê-lo porque sentem-se envergonhadas por carregar o pequeno prato com muita comida em público. E por que essa distinção entre implicação social e interação humano-produto é tão importante? Quando os designers projetam produtos, que mudam comportamentos, evidentemente existem razões para que a forma de comportamento desejada não é realizada normalmente, carecendo desta influência artificial do produto.

Um dos grandes problemas é o indivíduo não poder sempre priorizar as preocupações coletivas. O que é melhor para o coletivo – e, portanto, em média também para o indivíduo – nem sempre é sentida para ele como melhor ou é facilmente anulada por outras preocupações. Este é o principal motivo pelo qual vários indivíduos não se sentem atraídos por motivações coletivas, pois se não sentem a experiência individual de melhoria, por que a defenderiam? Este é provavelmente o principal sentimento de todo liberal ou de qualquer ser humano em mínimo desacordo com o Estado ou com qualquer obrigação coletiva. Tomemos como exemplo a sustentabilidade ambiental. Do ponto de vista social e de longo prazo, não é difícil conectar as preocupações coletivas com o comportamento desejável, como por exemplo ir para o trabalho de bicicleta ou em transporte público em vez de carro. No entanto, esse comportamento conflita com muitas preocupações, como desejo de conforto e eficiência. Se é difícil sentir diferença quando vários realizam certo comportamento ecológico, o que dizer da falta do sentimento de mudança quando um só tenta agir ecologicamente, separando tipos de lixo *v.g.*, ou quando um só terceiro o faz.

O poder do design está no seu potencial de tentar corrigir essas preocupações. Para muitos, a tarefa do designer é abordar preocupações individuais na interação com o produto, identificando as influências que podem ser desejáveis (TROMP; HEKKERT; VERBEEK, 2011). Os autores trazem o exemplo das campanhas para “se dirigir com o coração” projetadas por preocupação coletiva de segurança cujas preocupações individuais podem facilmente anulá-la. Já a lombada, diferentemente, foi projetada para obstruir comportamento irresponsável, ela danifica o carro quando o motorista não diminui a velocidade e, na maioria dos casos, as preocupações com a qualidade do carro e o aborrecimento em restaurar seus danos são maiores do que as preocupações sobre segurança ou responsabilidade social. A lombada funciona como uma punição para os indesejados comportamentos. Nos dois exemplos, a mesma motivação para alterar o comportamento é regulada externamente por algo. Essas intervenções que

explicitamente motivam a adoção de um estilo de direção mais responsável mostram como o design provoca o comportamento desejado de formas diferentes, como veremos abaixo, e molda as condições para respostas mais automáticas, até serem inconscientes e intrínsecas àquele ser humano.

Quadro 02 – Quatro tipos de influência baseadas nas dimensões de força e saliência.



(Fonte: TROMP; HEKKERT; VERBEEK, 2011, tradução nossa)

Baseado no Quadro 02, podemos classificar a experiência destas influências em força e saliência. Um design – de um artefato ou tecnologia – pode exercer influência que varia de fraca à forte (força) e de implícito a uma maneira mais explícita (saliência). Com base nestas duas dimensões, há quatro tipos de influência: coercitiva, persuasiva, sedutora e decisiva. Um produto pode coagir, persuadir, seduzir ou decidir por alguém. O design coercitivo é forte e aparente em sua influência, pois pessoas coagidas pelo design estão cientes da influência como uma força forte, como por exemplo o radar para desencorajar a condução rápida (TROMP; HEKKERT; VERBEEK, 2011). Essa perspectiva também se aplica à persuasão, embora a influência é experimentada como fraca (Quadro 02), pois geralmente é sem punição a não-conformadores e explícita em sua influência (por exemplo, uma campanha para promover alimentação saudável). O design sedutor já é fraco e implícito em sua influência, já que as pessoas raramente estão cientes da influência, como por exemplo o efeito de um micro-ondas em jantares em família. E o Design decisivo é forte e implícito, como a ausência de sofás e cadeiras em academias a fim de estimular a atividade física ou a ausência de janelas em casinos e shoppings para perda da noção de tempo de seus consumidores, logo, este design é o mais

perigoso – já que o sedutor não exerce tanta influência – porque o indivíduo geralmente não escolhe conscientemente conformar-se.

Somente o usuário que experimenta o design pode categorizá-lo como coercitivo, persuasivo, sedutor ou decisivo. Um engenheiro somente teoriza e espera. Essa categorização individual tem duas consequências. Primeiro, pessoas diferentes podem atribuir ao mesmo produto categorias diferentes, algumas pessoas experimentam uma câmera de velocidade ou os semáforos como persuasivos, outras como coercitivos. Em segundo, uma pessoa pode atribuir o mesmo produto a diferentes categorias ao longo do tempo. Uma pessoa pode – ser influenciada a – gastar sem pensar muito dinheiro depois de receber um cartão de crédito, mas pode também apenas tomar conhecimento dessa influência depois de ver o extrato do cartão de crédito. E por que são importantes estas diferenciações? Porque elas são também os parâmetros da internet. Estes quatro tipos de designs podem se misturar até no mesmo produto. Torna-se de mister importância notá-los para que, quando houver só um tipo de design de indução de certo comportamento socialmente desejável e ele não estiver sendo suficiente, se crie outros tipos de design que resolvam o problema de uma maneira melhor. Vejamos o caso dos usuários que estavam desrespeitando leis de direito autoral de doutrinadores. Não bastando para suprimirem as violações de direito autoral a influência coercitiva da lei e a influência persuasiva da moral de ser ruim utilizar algo alheio sem sua permissão, tiveram os técnicos – engenheiros da computação por demanda destes autores – que criar o arquivo pdf. protegido, ou seja, um novo design coercitivo para impedir o “Ctrl + c e Ctrl + v” de suas obras. Isto é, não bastaram os primeiros designs (o primeiro coercitivo-legal e o segundo persuasivo-moral).

Embora nunca garantam um resultado específico, certas estratégias aumentam as chances de se exercer uma influência particular desejável. O que pode ser especialmente proveitoso quando queremos uma influência particular para o benefício de toda coletividade. Tromp, Hekkert e Verbeek (2011) abstraem as seguintes estratégias principiológicas no design:

1. Criar uma barreira perceptível para comportamentos indesejados. Esta estratégia mostra e impõe ao usuário malefícios sobre certas ações, por exemplo o banimento de uma rede social por um comentário racista, seja por denúncias de outros usuários ou pela constatação de algoritmos da própria plataforma. Os psicólogos geralmente concordam que mudança comportamental duradoura só pode ser desenvolvida se um reforçador, em vez de punidor, segue consistentemente o comportamento. Embora muito eficaz, essa abordagem torna-se uma solução situacional e temporária e não leva, portanto, à mudança duradoura de comportamento, como um *troll* que não deixará de sê-lo por um só simples banimento. *Troll* é o ciberusuário

que provoca e enfrece, intencionalmente, outras pessoas envolvidas alguma em uma discussão, com comentários injustos e ignorantes, pelo mero prazer de causar algum sentimento ruim nesta outra pessoa.

2. Tornar evidente o comportamento inaceitável do usuário. Essa estratégia cria, às pessoas que cometem comportamento ilegal ou socialmente inaceitável, visibilidade pública ao aumentar a pressão social e complementa uma norma social já existente. Como o YouTube cessar o acesso a ferramentas de monetização do canal do podcaster Monark, após este defender que um partido nazista tem direito de existir. Costuma funcionar relativamente bem (quando ultrapassado um possível anonimato do usuário), apesar de, como dito muitas vezes, ser difícil calcular o quão uma ação é efetiva e boa enquanto influencia diferentemente cada pessoa.

3. Fazer certo comportamento uma atividade necessária para se fazer o uso de uma função do produto. Essa estratégia consiste em incluir um elemento de design que requer que o usuário execute um comportamento específico para alcançar seu objetivo final. No princípio, funciona bem. Contudo, assim que os usuários considerarem que o comportamento exige mais esforço do que eles estão dispostos a dar, a estratégia provavelmente falhará, como no exemplo de arquivos em pdf. protegidos para proteger direitos autorais os quais usuários conseguem desbloqueá-los para poderem copiar como querem ou como as amplamente divulgadas estratégias. Pela conversão online do arquivo em arquivo Word (.doc) ou uso da ferramenta “OCR” no menu “Editar”, escolhendo o modo “Texto editável” e o mesmo idioma do texto para realizar o OCR. Depois de realizar o OCR, um novo arquivo .pdf editável é aberto automaticamente. Outro caso são os juristas que, para copiar jurisprudências no JusBrasil, burla o seu código-fonte, por exemplo, no Firefox, bastando procurar a chave dom. event. clipboardevents. enabled e clicar duas vezes nela para mudar seu valor para false.

4. Fornecer ao usuário argumentos para um comportamento específico. Essa estratégia fornece ao usuário informações objetivas sobre as consequências de determinado comportamento, em uma espécie de reforço positivo. Estudos mostram que as pessoas preferem escolhas mais facilmente substanciadas por argumentos verbais, mesmo eventualmente, do que avaliar outras opções como melhores. Por exemplo, existem poucos benefícios de sair de casa para pagar contas enquanto um banco tem a possibilidade de pagamentos online com nenhuma taxa. O argumento da facilidade digital gera a adesão a este banco.

5. Sugerir ações. Essa estratégia propõe explicitamente certos comportamentos específicos, podendo se usar informações para fundamentar a sugestão, mas não é necessário. Quando o produto também fornece argumentos, visa alterar atitudes, como nos casos em que procura desencadear uma ação mais temporária e uma automática reação. Por exemplo, quando o Windows sugere ser atualizado ou até que compre uma nova versão prometendo certas melhorias de software, segurança e desempenho.

6. Acionar motivações diferentes para o mesmo comportamento. Essa estratégia adiciona uma função extra ao produto que provoca um reforço ao efeito desejado comportamento, gerando mais um benefício. Por exemplo, pagar com cartão de crédito porque além de poder pagar no crédito, com o benefício de postergar todos os pagamentos para o final de mês, ainda gerará milhas aéreas.

7. Eliciar emoções para desencadear tendências de ação. Essa estratégia tenta provocar uma emoção, geralmente a afeição, para seduzir pessoas a terem certas reações. Como as propagandas em rede social com imagens de africanos em estado de fome, induzindo o pagamento de ajudas financeiras pelo apelo a um comportamento mais empático. Também são recorrentes pessoas que passam por problemas de saúde pedirem, através de postagens em redes sociais, ajuda financeira a serem pagas, por exemplo, através da plataforma da Vakinha Online.

8. Ativar processos fisiológicos para induzir comportamento. Essa estratégia faz uso de processos fisiológicos humanos que resultam a partir de estados corporais, para que seja mais provável um específico comportamento ocorrer, ativando processos fisiológicos inconscientes. Há os óculos de 3 dimensões (3D) que geram até sensação de desequilíbrio em uma pessoa com simulações de uma montanha-russa, por exemplo, o que levaria a compra do produto pelo experimento de emoção. Outro exemplo é o da Coca Cola ou do Mc Donald's que, pelo extensivo aparecimento de suas marcas em propagandas, banners ou outdoors com produtos instintivamente apreciáveis e desejáveis, conseguem induzir vontade de comer ou beber nas pessoas ao verem seus logos já que a cor vermelha pode provocar emoções fortes (quase que agressivamente) e paixões intensas, aumentando a frequência cardíaca ao criar um senso de urgência e impulso, servindo a outras necessidades como a de obter lazer, pela Netflix; de ter notícias, pela GloboNews; ou de abastecer o carro, pela Texaco.

9. Desencadear tendências humanas para respostas comportamentais automáticas. Essa estratégia ativa uma tendência humana criando um estímulo perceptivo, instintivo ou aprendido. Trata-se de uma estratégia muito forte das principais empresas no mundo pela divulgação da imagem do seu logotipo a fim de gerar uma resposta – vontade – automática ou lembrança no indivíduo quando o mesmo sentir a necessidade do que certo produto sana. O indivíduo pode subentender que só certo produto sana por completo e com qualidade certa necessidade, praticamente toda propaganda tem este apelo. Este tipo de estratégia utiliza a experiência de reforço comportamental positivo e negativo.

10. Criar condições ideais para um comportamento específico. Essa estratégia projeta criar uma situação ideal para que o desejado comportamento ocorra “naturalmente”. Essa estratégia manipula as condições externas, mas não necessariamente interfere no comportamento psicológico subjacente. Um exemplo clássico no meio cibernético é a compra de todas empresas que dão certo em certo ramo para manter o monopólio, como a Google faz com sites de busca e softwares de aprendizagem de usuário, e inevitavelmente o usuário acabará utilizando “naturalmente” aquela plataforma sempre, pois será ela aquela com mais serviços ao usuário.

11. Fazer do comportamento desejado o único comportamento possível a ser executado. Essa estratégia transforma comportamentos diferentes do desejado em impossíveis. Quando essa estratégia é aplicada a desmotivados usuários, o comportamento é experimentado como regulado externamente. Como, por exemplo, no caso de redes sociais como Instagram e Facebook em que só é possível ver uma certa foto ou post de alguém, que não esteja no *feed*, ao abrir seu perfil. Logo, eles conseguem adicionar esta informação – como manifestação de suas vontades – ao perfil do usuário, gerando efetivos *ads*, propagandas na forma digital, e recomendações e, portanto, maiores lucros.

Assim, deliberadamente afetando o comportamento a fim de estimular específicas implicações, tais influências coletivas requerem uma redefinição do papel do engenheiro. Embora o designer nunca possa prever completamente todas as implicações sociais de seu produto ou serviço e embora o significado dos artefatos mude ao longo do tempo, essa realidade não necessariamente implica que os designers devem se abster de levar a sério as implicações sociais de seus projetos. Para Tromp, Hekkert e Verbeek (2011), os designers não podem mais se esconder atrás das necessidades e desejos dos consumidores. Em vez disso, devem assumir

a responsabilidade como modeladores de sociedade ao incorporar especialistas relevantes, como como sociólogos e formuladores de políticas, bem como cidadãos.

#### **1.4 INTERNET: EVOLUÇÃO HISTÓRICA E ATUAL REALIDADE**

*A internet é uma rede mundial de hardwares e softwares interconectados.*

A internet – o objeto, artefato e tecnologia que estudaremos – revolucionou e interliga constantemente o mundo comunicacional como nunca outra invenção. A internet é, de uma só vez, ao mesmo tempo e em qualquer lugar do mundo, um mecanismo de disseminação da informação e divulgação mundial. O contexto dos primeiros esboços e desenvolvimento de um computador fora durante a Segunda Guerra Mundial, onde Alan Turing tentou construir uma máquina para calcular a função Zeta de Riemann e encontrar soluções fora da linha crítica. As ideias de Turing e sua máquina Bombe permitiram generalizar esta função para decifrar qualquer mensagem da máquina alemã Enigma. Próximo ao fim da guerra, o time de Bletchley Park desenvolveu a máquina Colossus, para decodificar a cifra Lorenz, utilizada pelo alto-comando alemão. Os modelos estatísticos de Turing também foram fundamentais para a quebra da Lorenz. O Colossus foi a primeira aplicação com uso em larga escala de circuitos eletrônicos digitais.

A denominação de internet advém da junção das duas palavras do inglês *international network*. Traduzindo para o português, rede internacional. Assim, a internet é uma rede mundial de *hardwares* e *softwares* interconectados, pelos quais dados e informações são transmitidos a qualquer usuário conectado (CASTELLS, 2003, p. 13). Os primeiros registros de possíveis interações sociais por redes foram memorandos escritos por J. C. R. Licklider, do Massachusetts Institute of Technology (MIT), em agosto de 1962, ao pleitear o conceito da “Rede Galática”, prevendo a possibilidade de vários computadores serem interconectados globalmente pelo acesso instantâneo a dados e programas de qualquer posição geográfica. Um princípio básico bem semelhante com a internet de hoje. Licklider foi o primeiro gerente do programa de pesquisa de computador do DARPA, começando em outubro de 1962. Leonard Kleinrock, do MIT, publicou o primeiro trabalho sobre a teoria de trocas de pacotes em julho de 1961 e o primeiro livro sobre o assunto em 1964. No final de 1966, Roberts trabalhou no DARPA para desenvolver o conceito das redes computadorizadas e desenvolveu suas ideias para a

ARPANET, publicando em 1967. Em 1968, depois de Roberts e o grupo do DARPA terem refinado a estrutura e especificações para a ARPANET, uma seleção foi feita para o desenvolvimento de um dos componentes-chave do projeto: o processador de interface das mensagens (IMP). Na Conferência Internacional de Comunicação entre Computadores (ICCC), em 1972, Kahn coordenou uma exposição sobre a ARPANET. Essa foi a primeira demonstração pública desta tecnologia de rede.

Assim, a ARPANET amadureceu e se tornou a internet que hoje conhecemos. A internet foi fundada na ideia de múltiplas redes independentes interligadas, sendo a ARPANET pioneira nas trocas de pacotes de dados. Uma de suas grandes motivações foi o compartilhamento de recursos. Para isso, a internet incorpora um fundamento básico: rede de arquitetura aberta. Ou seja, a opção pela tecnologia em qualquer rede individual não é ditada por nenhuma arquitetura de rede particular ou pública e sim escolhida livremente pelo provedor, que a torna capaz de entrar em rede com outras redes pela “Arquitetura de Internetworking”. O desenvolvimento generalizado de *lanhouses*, PCs e estações de trabalho na década de 80 permitiu a prosperidade da internet. A tecnologia Ethernet, desenvolvida por Bob Metcalfe em 1973 é provavelmente a tecnologia de rede dominante.

A ARPANET fora segmentada em duas redes no início do ano de 1980. A MILNET que servia às necessidades militares e a ARPANET que suportava a investigação. O Departamento de Defesa coordenava, controlava e financiava o desenvolvimento de ambas redes. Em julho de 1977, Vinton Cerf e Robert Kahn realizaram uma demonstração do protocolo TCP/IP utilizando três redes ARPANET – RPNET – STATNET. Muitos consideram que foi esta a primeira demonstração do surgimento da internet. Apesar de responsável pelo início do desenvolvimento dessa rede, a tão mencionada ARPANET não foi a única colaboradora pela mesma como conhecemos hoje. O formato atual, segundo Castells (2003), também resulta de uma tradição de formação variada de redes de computadores que “no início da década de 1990 muitos provedores de serviços da internet montaram suas próprias redes e estabeleceram suas próprias portas de comunicação em bases comerciais. A partir de então, ela rapidamente cresceu como uma rede global de redes de computadores”.

Em 1989, fora criada a *World Wide Web*, popularmente conhecida como *web*, denominada pelo físico e pesquisador do MIT Timothy John Berners-Lee, que se traduz como “rede de alcance mundial”. Esta é a plataforma a qual viabilizou a internet que conhecemos. Assim, Morales Vilha explica que:

A *web* pode ser definida como um conjunto de recursos que possibilita navegar na Internet por meio de textos hipersensíveis com ‘hiper-referências’ em forma de palavras, títulos, imagens ou fotos, ligando páginas de um mesmo computador ou de

computadores diferentes. A *web* é o segmento que mais cresce na Internet e a cada dia ocupa espaços de antigas interfaces da rede. (MORALES VILHA, 2002, p. 20).

Leonardi (2005, p. 11), conceitua internet como “uma rede internacional de computadores conectados entre si. É hoje um meio de comunicação que possibilita o intercâmbio de informações de toda natureza, em escala global, com um nível de interatividade jamais visto anteriormente”. No artigo 5º do Marco Civil da Internet (MCI), a Lei n. 12.965, de 23 de abril de 2014, há a definição da internet como “o sistema constituído de conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”. Objetivamente, a internet é o conjunto de *hardwares* (como os servidores, *modems*, computadores, roteadores etc.) e *softwares* (*browser*/navegadores, aplicativos, *plug-ins* etc.) que interconectam, por meios de comunicação (linha telefônica, linha dedicada, fibra ótica, satélite, redes locais etc.), informações (na forma de dados) e acesso a variados serviços por meio, principalmente, de páginas de *websites* e de interfaces de aplicativos.

#### 1.4.1 No Mundo e no Brasil

*O apelo à ação estatal ressoa consistentemente.*

A priori vale ressaltar a inexistência de regras e políticas universais significativas para se combater crimes cibernéticos. A Convenção de Budapeste produz quase nenhum efeito para o Brasil. Hodiernamente, somente coexistem algumas iniciativas regionais. A União Europeia, União Africana, países do Caribe, Liga dos Estados Árabes têm regras comuns para enfrentar esse tipo de crime, por exemplo. Alguns ordenamentos são mais específicos, outros mais abrangentes e tão somente bases de princípios, como o caso do Brasil com o Marco Civil da Internet.

Observaremos dados importantes para demonstrar que as empresas não dão conta sozinhas das violações a dados por hackeamento, diferentemente do que muitos liberais gostariam de acreditar. Para se ter uma ideia da gravidade dessas violações, o custo médio, geralmente para uma empresa, de uma violação de dados (*data breach*) é de US\$ 3,92 milhões de dólares com uma média de 25,5 mil dados violados.

Uma violação de dados (*data breach*) é um evento no qual um nome do indivíduo e uma alguma informação pessoal são potencialmente colocados em risco, em formato eletrônico ou em papel, geralmente causados por ataques criminais, falha no sistema ou erro humano. Os custos de uma violação de dados variam de acordo com a causa e as salvaguardas em vigor no momento da violação dos dados. Nos EUA, uma violação custa mais, cerca de US\$ 8,19 milhões de dólares (IBM SECURITY, 2019, p. 3). E, geralmente, dois terços das violações ocorrem no primeiro ano da empresa e um terço nos anos seguintes (IBM SECURITY, 2019, p. 5). O tempo entre o momento em que ocorre um incidente de violação de dados e quando a violação é finalmente contida (também conhecido como ciclo de vida da violação) cresce constantemente. O tempo médio para identificar uma violação em 2019 foram de 206 dias e o tempo médio para conter uma violação foi de 73 dias, totalizando 279 dias. Isto representa um aumento de 4,9% no ciclo de vida da violação de 2018 (IBM SECURITY, 2019, p. 6). Aqui não defenderemos a exclusividade no Estado na guerra contra cibercriminosos, mas sim que podem e devem auxiliar neste combate. Das violações cometidas em 2019, 16% foram em entidades do setor público e grupos criminosos organizados estavam por trás de 39% das violações. Ademais, 71% das violações foram motivadas financeiramente e 25% pelo ganho de vantagem estratégica (espionagem). Por fim, 56% das violações levaram meses ou mais para serem descobertas (VERIZON, 2019, p. 5).

Corroborando com as percepções de Ellul, a solução é sempre mais tecnologias e técnicas de aperfeiçoamento e especializações de funcionários. A solução, logicamente porque a internet é inteiramente artificial, será sempre obter mais técnica. Em uma pesquisa da Ponemon Institute (2018, p. 1-2), 65% dos profissionais de segurança de TI entrevistados dizem que o envolvimento humano na segurança é importante na era da automação e 73% diz que a função de segurança de TI da sua organização era insuficiente. E sempre será. E ainda confirmando o tecnofilósofo francês, para 49% e 47% dos profissionais, a automação aprimora a capacidade de priorizar ameaças e vulnerabilidades e aumenta a produtividade do atual pessoal de segurança (PONEMON INSTITUTE, 2018, p. 3).

Para se ter uma melhor ideia, 59% das companhias americanas e britânicas experienciaram violações de dados através de um terceiro (PONEMON INSTITUTE, 2018, p. 3) e 53% das organizações experienciaram um ataque interno só no seu último ano (CROWD RESEARCH, 2019, p. 3). Os cibercriminosos focados no *ransomware* para a chantagem financeira começam a explorar outras oportunidades.

Só a empresa Symantec, a maior rede civil de inteligência de ameaças do mundo, bloqueia 142 milhões de ameaças diariamente em mais de 157 países. Na tecnologia de serviço

em nuvem, em 2018, mais de 70 milhões de registros foram roubados ou vazaram. Serviço de armazenamento em nuvem ou cloud é o empréstimo em *bytes*, cobrado financeiramente ou não, de seus servidores para guardar qualquer tipo de informação que o usuário queria guardar na rede. Isso é particularmente problemático para serviços em nuvem porque, embora instâncias da nuvem têm seus próprios processadores virtuais, eles compartilham conjuntos de memória; o que significa que um ataque bem-sucedido a um único sistema físico pode resultar no vazamento de dados de várias instâncias (SYMANTEC, 2019, p. 2-4). Tornar-se-á mais difícil para os invasores separar os recursos da empresa alvo dos provedores de nuvem e, ao mesmo tempo, será muito mais difícil para as empresas detectar um ataque a seus recursos nos estágios iniciais. A transição para a nuvem obscureceu os limites das infraestruturas da empresa. Como resultado, está se tornando difícil direcionar precisamente os recursos de uma organização. Portanto, conduzir um ataque se tornará mais difícil e as ações dos atores de ameaças se tornarão mais sofisticadas ou mais frequentes quando basearem-se no acaso e não no planejamento. Por outro lado, também será complicado para uma empresa identificar ataques direcionados em estágio inicial e separá-los da massa geral de ataques no provedor de internet. A investigação de incidentes se tornará mais complexa e, em alguns casos, menos eficaz. Os grupos de chantagem cibernética que coletam informações comprometedoras dos funcionários da empresa (por exemplo, evidências de crimes, registros pessoais e dados pessoais, como preferências sexuais) para fins de chantagem também se tornarão mais ativos no setor corporativo. Geralmente isso acontece da seguinte maneira: os atores de ameaças coletam e-mails e senhas vazados, encontram aqueles que são do seu interesse e filtram dados comprometedores que são posteriormente usados para chantagem ou ciberespionagem. Quanto mais fortes forem as especificidades culturais e os regulamentos regionais, mais rápida e eficaz será a alavancagem dos agressores. Como resultado, prevê-se que os ataques aos usuários para obter dados comprometedores aumentem (KASPERSKY LAB, 2019a), como vem sendo confirmado durante os anos. Nos dispositivos de IoT, a Symantec encontrou um aumento de 600% nos seus ataques globais em 2017 (SYMANTEC, 2018, p. 2). Internet das Coisas (IoT) é refere-se a uma rede de objetos físicos, geralmente os computadores, capazes de reunir e de transmitir dados e geralmente está associado à interação de todos aparelhos de uma casa.

A Kaspersky Lab (2019c), em 2019, viu 174 organizações municipais alvos de ransomware, um aumento de aproximadamente 60% em relação ao número de cidades vítimas de ataques no ano anterior. Ransomware é um método criminoso de extrair arquivos e dados pessoais e depois fazer chantagem para não serem divulgados. Enquanto nem todos confirmam a quantidade de fundos extorquidos e se um resgate foi pago ou não, a demanda

média por resgate variou de US\$ 5 mil dólares a US\$ 5 milhões de dólares e em média foi cerca de US\$ 1 milhão de dólares por vítima. Os números, no entanto, variaram bastante, pois os fundos extorquidos dos pequenos distritos escolares da cidade, por exemplo, às vezes eram 20 vezes menores do que os extorquidos das prefeituras dos grandes municípios. As entidades mais direcionadas eram organizações educacionais com 61% de todos os ataques de um número impressionante de 530 escolas; prefeituras e os centros municipais foram responsáveis por cerca de 29% dos casos; outro alvo popular foram os hospitais, responsáveis por 7% de todos os ataques. E por que isto ocorre? Em primeiro lugar, o orçamento de segurança cibernética dos municípios geralmente se concentra mais em seguros e respostas a emergências do que em medidas de defesa proativas. Isso resulta em casos em que a única solução possível é pagar aos criminosos e facilitar suas atividades. Ellul bem diria que isto é motivo de o ser humano tão somente tentar alcançar os avanços da técnica, mas nunca dominá-la. Em segundo lugar, os serviços municipais costumam ter inúmeras redes que incluem várias organizações e, portanto, atingi-los causa interrupções em vários níveis ao mesmo tempo. Esta é a clássica característica técnica já mencionada, a unicidade. Além disso, os dados armazenados nas redes municipais costumam ser vitais para o funcionamento dos processos cotidianos, pois dizem respeito diretamente ao bem-estar dos cidadãos e das organizações locais. Ao atingir esses alvos, os cibercriminosos estão atingindo um ponto sensível. Por ser misantropa, a técnica não liga para a sensibilidade do ser humano, ao contrário, ela abusa, explora e, cada vez mais, mostra que a sensibilidade e mentalidade subjetiva humana são seus pontos fracos, os mais fáceis de serem explorados, levando o ser humano inconscientemente a crer que este lado emocional e vulnerável é sua ruína.

Outra vulnerabilidade que temos hodiernamente é a tecnologia 5g, que se espera que seja 100 vezes mais rápido que os atuais sistemas de 4ª geração (4g). Mas como sabemos, quanto maiores as tecnologias, maiores as preocupações. À medida que as inovações 5g se espalham, mais deficiências e imperfeições aparecerão nos equipamentos 5g, nas estruturas dos clientes e na administração pelas autoridades. O 5g, com seu curto alcance, significará definitivamente mais torres de comunicação celular sendo implantadas em centros e edifícios comerciais. Com o conjunto de ferramentas certo, alguém poderia rastrear a localização precisa dos usuários. Provedores de serviços 5g também terão amplo acesso a grandes quantidades de dados enviadas pelos dispositivos do usuário, o que poderia mostrar exatamente o que está acontecendo na casa de um usuário e, no mínimo, descrever através de metadados seu ambiente de vida e seus sensores internos, explorando a IoTs. Esses dados podem expor a privacidade de um usuário ou podem ser manipulados e mal utilizados. Lúdica e alegoricamente, há o episódio

“Atendimento Automatizado ao Cliente” (2021) da série “Love, Death + Robots” em que os aparelhos domésticos das casas se rebelaram contra seus donos. Os provedores de serviços também podem considerar vender esses dados para outras empresas de serviços a fim de propagandas melhores direcionadas. Em alguns casos, as vulnerabilidades podem causar problemas de saúde, por exemplo, se os aparelhos terapêuticos de um cliente forem desconectados e não estiverem operacionais. As ameaças em potencial serão ainda maiores quando componentes críticos de infraestrutura, como equipamentos de água e energia, forem colocados em risco (HASBINI, 2019).

Em 2019, só as soluções da Kaspersky (2019b, p. 3) repeliram quase 1 bilhão de ataques lançados online e 270 milhões de URLs únicos (sites criados por pessoas e por algumas espécies de IA e bots) foram reconhecidos como maliciosos por antivírus da web. Quanto ao Estados e às empresas no combate aos cibercrimes, as organizações geralmente veem, na regulamentação do governo, eficácia limitada no auxílio ao gerenciamento de risco. Vejamos que só 28% das empresas consideram regulamentos governamentais como muito eficaz na melhoria da segurança cibernética e 37% das empresas consideram os padrões das próprias empresas como muito eficaz na melhoria da segurança cibernética. Já quanto às preocupações, 54% das pessoas sentem-se altamente preocupadas sobre ataques cibernéticos no Estado e ainda 55% disseram que o governo precisa fazer mais para proteger organizações contra ataques cibernéticos no Estado. Globalmente, na opinião das empresas, 79% dos entrevistados classificaram riscos cibernéticos como uma das cinco principais preocupações de sua organização, contra 62% em 2017, e sua preocupação como número 1 quase quadruplicou, de 6% a 22%. Estimou-se o custo anual do cibercrime em 2019 em US\$ 1 trilhão. As organizações podem ficar frustradas quando seus aumentos do investimento em mitigação de riscos cibernéticos não diretamente se correlacionam a melhores resultados, como geralmente ocorre com outras áreas de investimento empresarial (MARSH, 2019, p. 2-6). O que é um grande problema, pois não basta conhecê-lo, nem vaciná-lo, é preciso erradicá-lo e quando o fazem no tempo médio de 279 dias, multiplicam-se neste tempo a quantidade de outros problemas e danos.

Empresas veem eficácia limitada da regulamentação do governo para ajudar a gerenciar risco cibernético, mas, mesmo assim, desejam ajuda com os desafios cibernéticos que elas próprias não podem efetivamente resolver sozinhas. Nos últimos anos, os reguladores adotaram globalmente inúmeras medidas para responsabilizar as corporações e executivos por garantir uma cibersegurança eficaz e uma manutenção dos dados dos clientes em segurança. Muitos desses regulamentos e estruturas legais exigem um maior grau de transparência – *accountability* – das organizações em todos os níveis de suas atividades de manipulação de dados e em sua

prontidão para gerenciamento de riscos cibernéticos. Poucas empresas acreditam que a regulamentação do setor é eficaz para ajudar a melhorar a postura de segurança cibernética de sua própria organização. Indústrias altamente reguladas, como aviação, instituições financeiras e comunicações, eram mais propensas a valorizarem mais o governo diante da regulação do risco cibernético. Consistente com essa visão, 55% das organizações viram a necessidade de que os governos façam mais para proteger as empresas privadas de ataques cibernéticos no Estado (MARSH, 2019, p. 20-21). O apelo à ação estatal ressoa consistentemente em todas as regiões, com a maior resposta positiva entre instituições financeiras e organizações de serviços profissionais. Esses resultados mostram que, embora as empresas geralmente prefiram uma abordagem não prescritiva para gerenciar sua segurança cibernética e segurança cibernética, a atividade do Estado é uma clara exceção.

No ano de 2015, por exemplo, a Kaspersky Lab (2019b, p. 3) registrou mais de 398 milhões de ataques de *malwares* na América Latina. Além disso, a empresa de segurança detectou que, durante este período, em cada 100 tentativas infecção, mais de 82% ocorreram *offline*, isto é, por meio de USB contaminados, pela pirataria de softwares ou quaisquer vias as quais não exigem em princípio o uso da internet para a primeira contaminação do conteúdo malicioso. Outros 18% são de ataques cibernéticos conectados à internet. De acordo com Bestuzhev (2016), quase 50% dos usuários online do Brasil sofreu uma tentativa de golpe nos seus últimos 12 meses. Um impressionante número. Ou seja, o perigo não é só através da internet, mas também majoritariamente pelos hardwares infectados.

Como vimos, pequenas empresas enfrentam desproporcionalmente – porque existem gastos fixos – maiores custos comparados a maiores organizações. O custo total para as maiores organizações (de mais de 25 mil funcionários) foi em média de US\$ 5,11 milhões, o que significa US\$ 204 por funcionário. Organizações menores com entre 500 e 1.000 funcionários tiveram um custo médio de US\$ 2,65 milhões ou US\$ 3.533 por funcionário. Assim, organizações menores têm custos mais altos em relação ao seu tamanho e orçamento que maiores organizações, prejudicando sua capacidade de recuperação financeira do incidente (MARSH, 2019, p. 7), justamente por não terem condição de investir tão bem em proteção virtual, enaltecendo mais ainda a importância da tutela estatal nestes casos. Outro dado que confirma tal necessidade foi a probabilidade de uma violação envolvendo um mínimo de 10 mil registros ser estimado em aproximadamente 29,6% em 24 meses e a chance de uma violação de dados envolvendo um mínimo de 100 mil registros ser de aproximadamente 1,2% (IBM SECURITY, 2019, p. 48). Qualquer empresa tem que estar em alerta já que a probabilidade de

experimentar uma violação de dados nos seus próximos dois anos é de 29,6% (IBM SECURITY, 2019, p. 46).

Uma outra informação impactante é que 68% dos arquivos perdidos por resultado de ciberataques são declarados irrecuperáveis. Antes havia uma média de 170 dias para se detectar e eliminar o malicioso ataque (DASCALESCU, 2018) em 2016, quando em 2019 a média foi de 279 e só tende a aumentar. Porém, o dado com o maior número de conteúdo prejudicial é o dos *spams*. Estima-se um total de 28 bilhões de *spams* enviados em e-mails por dia. Uma taxa de spam global em média de 60%, sendo 1 em cada 965 um *phishing*. Ainda, de acordo com a Symantec, meio bilhão de informações pessoais foram roubadas ou perdidas em um só ano (SYMANTEC, 2019, p. 5)

Já no Brasil, o crime cibernético mais comum é a fraude bancária online. O Brasil está em segundo lugar em relação a crimes dessa natureza, depois da Rússia. Diariamente, são registrados 366 crimes cibernéticos em todo o país. Em 2018, a SaferNet Brasil, com o Ministério Público Federal (MPF), contabilizou 133.732 queixas de delitos virtuais. Ou seja, houve um aumento de 110% em relação à 2017 (SAFERNET, 2018). Os principais delitos no campo de internet no Brasil acontecem no âmbito da injúria, calúnia, difamação, pornografia infantil, misoginias e preconceitos, roubo de informações, estelionato, golpes em apps e subtração de valores.

Explica Leandro Turbino, diretor de Vendas do Micro Focus Brasil, que para as empresas brasileiras, os processos ainda são vistos como um fardo para a concessão de acesso e difíceis de auditar e validar mudanças. No Brasil, entrevistados indicaram que a razão mais importante para as organizações estarem em risco era a falta de políticas de gerenciamento de acesso e de aplicação das políticas que estão em vigor. Além disso, o aspecto mais difícil nesta política é a revogação nos privilégios de acesso quando o trabalho de um funcionário é encerrado. Já o analista sênior da Kaspersky Lab (2017) no país, Fábio Assolini afirma que:

Cerca de 95% dos programas maliciosos desenvolvidos no Brasil visam o roubo de credenciais de Internet Banking e números/senhas de cartões de crédito. Além disso, vimos cibercriminosos explorando e buscando novas maneiras de enganar os internautas. Por este motivo é essencial a prevenção para realizar transações financeiras online ou interagir com comunicados enviados pelos bancos. Recomendamos fortemente que todos os usuários tenham uma solução de segurança para se proteger e evitar essas perdas.

O delegado Stênio Santos, Chefe do grupo de repressão a crimes cibernéticos da Polícia Federal (PF-DF), afirmou ver o crescimento dos crimes digitais no Brasil como um fenômeno natural diante da popularização do acesso à tecnologia e da implementação de novas

tipificações desses crimes a partir de legislações como a Lei Carolina Dieckmann. De acordo com ele (MATSUURA; JANSEN, 2015), o perfil do cibercriminoso é variado:

Percebemos que alguns cibercriminosos nem mesmo têm profundo conhecimento de tecnologia. São pessoas que adquiriram um vírus criado por um *hacker* de verdade e, a partir daí, viram a oportunidade de ganhar dinheiro sem esforço. Claro, há também os *hackers* extremamente capazes que comercializam as ameaças que criam e as informações sigilosas que conseguem. [...] Devido ao problema carcerário do país, nosso Judiciário tende a optar por penas alternativas. Em geral, esses crimes cibernéticos não são praticados com grave ameaça ou violência, o que faz com que a pessoa, num primeiro momento, não fique presa. [...] Quando o crime é de fraude bancária e de pornografia infantil, temos percebido a reincidência. Muitos criminosos sentem ser mais vantajoso praticar o ilícito, ser preso, sair e voltar a praticar o cibercrime do que buscar um emprego formal.

Paralelamente a isso, os ataques são recorrentes devido ao baixo grau de informação de que a população dispõe quanto aos riscos digitais, logo, “segurança digital, assim como educação sexual e cidadania, é um tema que atualmente deveria ser abordado nas escolas, porque o mundo hoje é digital. Há uma falha grande no Brasil nesse sentido, porque esse tipo de educação não é feito” (MATSUURA; JANSEN, 2015). De acordo com Norton (2012), a cada 13 segundos um brasileiro é vítima da tentativa de fraude com documentos roubados ou informações furtadas da internet, sendo 28 milhões de brasileiros já atingidos. Ameaças e cibercrimes custam cerca de R\$ 16 bilhões de reais anualmente ao país.

#### 1.4.2 Insuficiência das Empresas

*Os hackers e malwares se movem rapidamente; já as defesas, não.*

Como constatado, empresas em escala global não conseguem acompanhar os avanços e as demandas do mercado da internet. Em termos de proteção dos dados de consumidores, estes apenas se dão por conta da inexistência desta proteção em decorrência de um evento danoso que interfere na sua privacidade. Na realidade real-virtual em que o mundo se encontra, a exploração de vulnerabilidades de softwares é um dos principais alvos de ciberataques, com diferentes técnicas ganhando impulso. Assim como em 2014, as 10 principais vulnerabilidades exploradas em 2015 eram conhecidas há mais de um ano, com 68% tendo sido reportadas há três anos ou mais. Ou seja, novamente é constatado que não é necessariamente a falta de informação do problema e sim a capacitação de empresas na solução do mesmo. Por exemplo, 29% de todos *exploits* bem-sucedidos de 2015 permaneceram utilizando o *Stuxnet* 2010, que

havia sido “corrigido” duas vezes (HPE SECURITY RESEARCH, 2016, p. 30-33), mostrando que até quando tentam solucionar, há meios alternativos para se utilizar de vias ilícitas já corrigidas.

Os hackers e *malwares* se movem rapidamente; já as defesas, não. O tempo de reação não aumentou e não há previsão que aumentará a um ritmo equivalente. Os atacantes exploram essas vulnerabilidades muito mais rápido que os provedores podem criar e implantar *patches*. Os invasores também se aperfeiçoaram, tornando cada ataque mais seletivo por infectar sites legítimos, monitorando sites de visita e visando apenas as empresas que querem atacar. Para complicar ainda mais a capacidade das empresas de se defenderem, apareceram as atualizações de software *trojanized*. Atacantes identificam programas de softwares comuns usados por organizações alvo, escondem seus *malwares* dentro de atualizações de software para esses programas e, em seguida, esperaram pacientemente que os seus alvos baixem e instalem o software, fazendo com que as empresas se autoinfectassem.

No ano de 2014, sessenta por cento de todos os ataques direcionados atingiu organizações de pequeno e médio porte. Como visto, essas organizações têm menos recursos para investir em segurança e ainda não estão adotando as melhores práticas básicas como bloquear arquivos executáveis e anexos de e-mail *screensaver* (HPE SECURITY RESEARCH, 2016, p. 30-33). Isso coloca as empresas, seus parceiros de negócios e, naturalmente, seus consumidores em maior risco. Medidas preventivas são caras e difíceis de se notar resultados quando possuem estas empresas outras prioridades de investimentos. Quase nenhuma empresa, seja grande ou pequena, está imune.

Outro relatório, da Micro Focus em parceria com o Instituto Ponemon, anunciou os resultados de um novo estudo global focado em explicar o porquê da inovação empresarial e segurança muitas vezes não andarem juntas, pelo contrário podem ser motivações antagônicas. A pesquisa demonstra que, na maioria das vezes, as organizações sabem das mudanças em operações de TI e o que melhorar na segurança, ou seja, novamente vemos que não se trata de falta de informação quanto ao problema. Todavia, devido às pressões de mudança de negócios, transições e demandas de mercado e adoção de novas tecnologias, as organizações sacrificam a segurança pela velocidade dos negócios (PONEMON INSTITUTE, 2016, p. 3).

Altas demandas no vasto mercado necessitado de capacitação estão gerando consequências que impactam o meio digital e a entrada de empregados incapacitados é uma delas. Alguns resultados importantes revelam que: 62% dos respondentes disseram que não podem manter a informação segura; 44% acreditam que o processo de concessão de acesso é oneroso; 64% dizem que a informação do cliente está em risco por causa de controles de acesso

fracos; 47% dizem que há um risco para a informação do empregado, como resultado de controles de acesso fracos; e 49% acreditam que a internet das coisas é uma tendência importante que afeta o gerenciamento de identidade e acesso (PONEMON INSTITUTE, 2016, p. 3). Estamos na necessidade de profissionais de segurança cibernética. Enquanto os riscos do aumento da digitalização só crescem (como os dados em *cloud*, aplicações corporativas e a *Internet of Things*), o número de profissionais de segurança cibernética permanece crescendo a num nível baixíssimo, criando a pior vulnerabilidade possível para as empresas: a falta de profissionais de TI qualificados. Em estudo recente, estima-se que cerca de um milhão de especialistas estão em falta no mundo, incluindo especialistas que deveriam ser líderes neste setor. 82% das pessoas que tomam decisões para a segurança cibernética em empresas acreditam que há uma falta de conhecimento e 71% estão convencidos de que este déficit de especialistas é parcialmente responsável pelos ataques cibernéticos que estão constantemente atacando corporações.

Ou seja, há extrema insuficiência de empresas do mundo todo, não só evidenciado por este estudo, mas por todas referências trabalhadas neste reverente trabalho. Em diversas áreas no meio digital, necessidades são demonstradas diariamente. Empresas, em âmbito mundial, não conseguem sozinhas manejar todos requisitos de segurança. A internet tem diversas complexidades e multifacetadas, as quais empresas não conseguem, nem de modo satisfatório para a segurança geral, compreendê-la e principalmente assegurá-la para seus consumidores dentro da constante dinâmica digital. Neste contexto, medidas públicas e regulamentação do Estado são necessárias, com a profissionalização e organização das ações contra hackers e melhores agências e sistematização de atores públicos no combate real ao cibercrime. A insuficiência das empresas não é algo momentaneamente epidêmica, na verdade, persistirá em larga escala. Um dos principais motivos é a tendência de empresas, na sua designação de meio para obtenção de lucro, em solucionar tão somente os problemas que mais as afetam mais economicamente. Havendo epidêmicos ataques cibernéticos, por falta de preocupação profissional e retorno monetário (em que as pequenas e médias empresas são as mais atingidas), surge uma necessidade imperiosa na resolução destes conflitos por parte do Estado.

A quem se deve dar a atribuição de resolver problemas computacionais os quais grades empresas não conseguem ou não se preocupam em solucionar, prejudicando usuários diretamente? Quem deve, de maneira organizada, recolher dados, operacionalizar soluções e formar uma integralização dos *patches* para combate à *malwares* para todas as empresas do país, solidarizando soluções para um progresso conjunto? Quem deve se preocupar com a insuficiência de pequenas e médias empresas na sua proteção de dados na proteção de dados

dos consumidores-cidadãos, sancionando descumprimentos e descasos? Quem deve se preocupar com usuários que não necessariamente usam a internet pelos cuidados de uma empresa e formar uma série de procedimentos a serem tomados pelo meio privado, diagnosticando problemas e estabelecendo metas, sempre de maneira a atingir o menos possível o aspecto financeiro das empresas? Quem deve desenvolver uma especialização na área e reparar uma carência constante no mercado digital e realmente compreender e, principalmente, assegurar a internet – complementando a consolidação de direitos humanos – para seus usuários dentro da dinâmica atual e constante digital, de forma geral, satisfatória, organizada, solidária, integralizada e, especialmente, imparcial? Numa visão totalmente liberal, deveriam ser tão somente as empresas, as quais já se encontram hoje num ambiente digital praticamente liberal e nem satisfatoriamente solucionam os *malwares* e, em geral, tampouco protegem os usuários. Numa visão realista, deve ser o Estado este consolidador, de forma colaborativa, dos direitos humanos e constitucionais tão atacados no meio digital. O meio privado pode e deve se adaptar e remediar o máximo de *malwares* os quais lhe forem acatados. Porém, no contexto de extrema globalização, a incessável adaptação dos *malwares* e hackers deve obter uma investida estatal.

Mediante a regulamentação do mercado no tratamento de dados de acordo com a LGPD, no Brasil hoje existe a obrigatoriedade de comunicar os incidentes, mas isso não impede que, no contexto digital totalmente aleatório, o caos cibernético facilmente se instaure. Sendo assim de mister importância a realização de políticas públicas como instâncias de acesso e de bem-estar social, de forma organizada e colaborativa. Apesar de ser atrativa a noção de internet como meio anárquico-liberal, ela somente deve prosperar na medida em que não atinja o próximo e para assegurar o respeito aos limites da liberdade e da privacidade, o Estado deve regulamentar e proteger seu consumidor-usuário.

Para exemplificar outros casos da vasta insuficiência empresarial no ramo digital, temos em seguida problemas empresariais de âmbito internacional. A maioria das violações ocorre na América do Norte. Estima-se que o custo médio de uma violação de dados seja superior a US\$ 150 milhões (JUNIPER RESEARCH, 2019), com previsão de custo anual global de US\$ 2,1 trilhões (EXPERIAN, 2014). Estima-se que apenas no primeiro semestre de 2018, cerca de 4,5 bilhões de registros foram expostos como resultado de violações de dados (GEMALTO, 2018). Em 2019, uma coleção de 2,7 bilhões de registros de identidade, composta por 774 milhões de endereços de e-mail exclusivos e 21 milhões de senhas exclusivas, foi publicada na web para venda (HUNT, 2019).

Temos um ranking de dados com a empresa, ano da violação e quantidade de dados mais motivo, respectivamente: Yahoo, 2013, 3 bilhões de contas através de uma ação hacker

(PERLROTH, 2017); vários websites chineses, 2019, 2,7 bilhões de e-mails e senhas (BISCHOFF, 2019); First American Corporation, 2019, 885 milhões através de segurança ruim (KREBS, 2019); Facebook, 2019, 540 milhões também por má segurança (UPGRUARD CYBER RISK, 2019); Marriott International, 2018, 500 milhões de dados hackeados (PERLROTH; TSANG; SATARIANO, 2018); Yahoo, 2014, 500 milhões de dados hackeados; Friend Finder Networks, 2016, 412 milhões de dados hackeados por má segurança; TrueCaller, 2019, 300 milhões de dados (SARMAH, 2019); Microsoft, 2019, mais de 250 milhões de dados expostos por desconfigurações (BISCHOFF, 2020a); Facebook, 2019, mais de 267 milhões de dados por má segurança (BISCHOFF, 2020b). E estes são só alguns. São milhões de dados de milhares de empresas sendo violados mensalmente.

Só a empresa Facebook, hoje Meta, foi multada em US\$ 5 bilhões pela Comissão Federal de Comércio dos EUA (FTC) para resolver as preocupações de privacidade com o escândalo do desvio de dados da Cambridge Analytica. O famoso caso que influenciou – não é possível saber se também decidiu – os resultados da eleição presidencial americana de 2016. Houve ainda o caso em que cerca de 90 milhões de pessoas tiveram que fazer login novamente no Facebook ou em qualquer um dos aplicativos que usam seu login pelo vazamento de dados (ROSEN, 2018). Outros mais de 540 milhões de registros sobre usuários do Facebook foram expostos publicamente no serviço de computação em nuvem da Amazon. Um relatório divulgado pela UpGuard (2019) demonstrou que dois desenvolvedores de aplicativos do Facebook publicaram os registros à vista, causando mais uma importante violação de dados para a maior rede social do mundo. O Facebook somente avisa seus usuários das violações anos depois. Oficialmente, como de praxe, empresas provedoras têm intransparência com seu consumidor-usuário para não prejudicar o valor de suas ações na bolsa de valores e, por isso, o Facebook muitas vezes não fala sobre o assunto. Lembrando que cerca de 600.000 contas no Facebook são comprometidas todos os dias (DASCALESCU, 2018).

Relatos como os de Frances Haugen não deveriam ser surpresas. Ela era uma engenheira norte-americana, ex-gerente do Facebook e divulgou dezenas de milhares de documentos internos da empresa à Comissão de Valores Mobiliários dos Estados Unidos (SEC) e ao Wall Street Journal em 2021 (HORWITZ, 2021). Houve relatos de isenções para usuários de alto perfil, impactos na juventude, impactos de suas alterações de algoritmo de 2018, o Facebook otimizar seus próprios interesses em detrimento do que era bom para o público, fraquezas na resposta a: tráfico de pessoas, cartéis de drogas, desinformação política, discurso de ódio, saúde mental de adolescentes, tráfico de pessoas, promoção de violência étnica, tratamento preferencial para determinados usuários, desinformação de vacinas e suas

comunicações com investidores, dentre outros problemas. Estes documentos internos do Facebook enviados por Haugen contradizem o testemunho de 2020 do Zuckerberg, que já citamos, perante o Congresso dos EUA.

Como vimos, o Yahoo é o campeão de violação de dados. Citamos o assombroso caso de 2013 onde estima-se que os dados de todos seus usuários foram violados, cerca de 3 bilhões. Ele informou no dia 22 de setembro de 2016 um vazamento de informações, por atividade criminosa do hacker Peace, atingindo pelo menos 500 milhões de usuários sem evidências de patrocínio de algum país. Entre as informações roubadas, estariam nomes, endereços de e-mail, números de telefone, datas de nascimento, perguntas de segurança e dados de registro de senhas. O Yahoo já havia anunciado que investigava a suposta invasão deste hacker, que dizia ter desde 2012 dados pessoais de cerca de 200 milhões de usuários. Este mesmo hacker vende abertamente os dados pessoais, contas de e-mail e senhas na dark, podendo-se encontrar o site de leilão facilmente ativo na dark web. No mesmo Mercado negro – TheRealDeal – deste mesmo hacker, Peace\_of\_Mind, em 2016 incluía-se 67 milhões de contas de usuário do LinkedIn, 360 milhões do MySpace, 68 milhões do Tumblr, 100 milhões do site da mídia social russa VK.com e, mais recentemente, outros 71 milhões do Twitter (GREENBERG, 2016); estes números hoje são muito maiores.

Já o *Dropbox*, um dos mais populares serviços de armazenamento em *cloud*, divulgou que teve 68 milhões de senhas de acesso e endereços de e-mail hackeados na internet em 2012. Segundo a empresa, os dados foram divulgados no ano de 2016, 4 anos depois, quando a base de dados das informações dos usuários foi encontrada pela empresa de segurança Leakbase. Na época, a empresa havia informado a seus clientes que apenas os endereços de e-mail tinham sido vazados, subestimando o impacto do incidente. A companhia, com um atraso de 4 anos, disse que não tinha conhecimento de toda a extensão do roubo de senhas. E mesmo mediante tamanho lapso temporal de conhecimento da empresa, a *Dropbox* disse que não havia “nenhuma indicação de que as contas de usuários foram indevidamente acessadas” (HEIM, 2016, tradução nossa). Infelizmente, é comum esta atitude de apaziguamento dos clientes das empresas, omitindo o real perigo e impacto que estiveram, com falta de honestidade na divulgação da real situação que se passa uma empresa quando hackeada. Na lógica de mercado, a omissão de informações as quais os usuários têm o direito de saber é simples consequência da busca empresarial ao máximo lucro, atropelando direitos dos consumidores.

Em 2014, ao analisar 6,3 milhões de *apps*, a Symantec descobriu que 17% de todos os aplicativos do *Android* (quase um milhão no total) eram, na verdade, um *malware* disfarçado. Além disso, os aplicativos *grayware* (quase 2,3 milhões), que não são maliciosos por design,

mas praticam ações prejudiciais como identificação comportamento do usuário, eram 36% de todos os aplicativos móveis. Ainda, encontrou-se 46 novas espécies de *malwares* em dispositivos *Android*, um pouco menos do que as 57 encontradas em 2013, chegando a 277 espécies de *malwares* em 2014. Em uma pesquisa, um em cada quatro admitiram que não sabiam o que eles concordaram em dar acesso em seu telefone quando faziam o download de um aplicativo. E 68 por cento estavam dispostos a trocar sua privacidade para nada mais do que um aplicativo gratuito (SYMANTEC, 2015).

De acordo com o estudo da Kaspersky Lab (2015), *Are you cyber savvy?*, mediante dados de 18 mil consumidores globais sobre seus hábitos na internet, foram descobertos números consideráveis de usuários os quais expõem suas privacidades e até dados pessoais em seus telefones às ameaças virtuais devido principalmente à instalação de aplicativos sem a segurança devida. Alguns *apps* podem afetar a privacidade do usuário, iniciar a instalação de outros programas ou até mesmo alterar a configuração do sistema operacional de um smartphone, já que o usuário autorizou – sem saber – estes acessos durante o processo de instalação. O estudo mostrou que quase 40% dos brasileiros correm risco, pois não têm conhecimento técnico adequado para limitar as permissões dos aplicativos ao instalá-los; que 12% deles não delimitam as ações dos aplicativos em seus aparelhos; que 20% dão permissão aos aplicativos displicentemente; que quase 40% dos brasileiros não se importam com o contrato de licença de instalação do aplicativo, sendo que quase 15% nem leem as mensagens de instalação. Ainda mais, um quarto de todos funcionários mentem e omitem quando cometem erros na empresa sobre segurança de informação. Mas sabemos que o último número é, na realidade, maior.

Portanto, até quando as permissões do aplicativo não são preenchidas, ele pode acessar de forma legal os dados pessoais e privados contidos nos dispositivos móveis, como informações de contatos, localização e até fotos. Não se tem conhecimento do contrato que estão aceitando quando não leem as mensagens durante o processo de instalação. Ou seja, se clica em “aceito” sem saber o compromisso que está assumindo, assinando, assim, um contrato sem ler suas cláusulas. E isto traz sérios problemas. Falaremos mais à frente sobre este consentimento quase-tácito sobre os Termos e Condições de aplicativos e provedores.

Outros casos mais recentes são: da British Airways, multada em US\$ 230 milhões, por uma violação de aplicativos móveis que comprometeu cerca de 380 mil pagamentos com cartão; da Under Armour, que sofreu uma violação de dados que afetou 150 milhões de usuários de suas contas MyFitnessPal, as ações da empresa caíram imediatamente 3,8% (demostrando aqui o empecilho para estas empresas divulgar estas informações); da Timehop, que sofreu uma

violação que expôs nomes e e-mails de cerca de 21 milhões de usuários; e da 7-Eleven Japan, que suspendeu o recurso de pagamento móvel do aplicativo 7Pay depois que os invasores exploraram uma função de redefinição de senha para cobrar fraudulentamente US\$ 500 mil em compras (SCHURR, 2019).

Estes dados são obtidos através do hackeamento direto ao sistema digital integrado destas empresas ou pelo descuido de empregados que instalam involuntariamente um malware. Mas existe também um terceiro contexto. Especialmente no caso do hacker Peace, poderia ter ele um altíssimo conhecimento, mas também vários desses dados podem ter sido obtidos através de vendas ilegais por seus próprios empregados. E geralmente a solução neste caso é a constante mecanização deste meio com a progressiva desnecessidade do ser humano. Podemos constatar esta corruptibilidade também na pirateação de canais, onde a maioria dos fornecedores deste serviço, com o fornecimento do aparelho desbloqueado de captação dos canais, são funcionários ou ex-funcionários dos próprios provedores de canais de TV fechada.

#### 1.4.3 Monetização de Malwares

*O lucro é o ponto crucial de todo scam.*

Neste contexto, houve uma evolução do perfil dos cibercriminosos, ao deixarem de lado os golpes genéricos e aleatórios para ataques mais direcionados e com objetivos definidos, como o ganho financeiro. Soma-se a este fator o aumento da inclusão digital através de diferentes dispositivos, possibilitando novas e diferentes armadilhas. O *malware* começou como diversão e tornou-se uma atividade geradora de lucro para hackers.

O *Ransomware* é um modelo de ataque cada vez mais bem-sucedido, com vários grupos causando devastação ao criptografarem arquivos de consumidores e usuários corporativos e pedir uma recompensa para descriptografarem. Alguns exemplos são o *Cryptolocker*, *Cryptowall*, *CoinVault*, *BitCryptor*, *TorrentLocker*, *TeslaCrypt* entre outros. Os ataques de *malwares* a caixas eletrônicos usam hardware, software carregado no caixa eletrônico ou uma combinação dos dois para furtar informações sobre cartões de crédito. Em alguns casos, os ataques no nível de software passam por cima da autenticação dos cartões para fornecer dinheiro diretamente. Cavalos de Tróia voltados a bancos, como variáveis do *Zbot Trojan*, continuam a ser problemáticos apesar dos esforços de proteção. Dentre as ofertas no mundo cibercriminoso, o *malware* bancário dispara na frente devido à popularidade do Internet Banking no país onde

40% da população brasileira realizou operações bancárias online em 2014, por exemplo. Por meio do *malware* kaiser, sempre que o usuário de um sistema infectado visitava o site de um dos bancos-alvo, eram registradas as teclas digitadas. Os cibercriminosos, então, ganham acesso aos números da conta bancária. Por R\$ 5 mil, os compradores podem registrar as teclas digitadas de até 15 sites e têm acesso a serviços de suporte 24 horas (NORTON, 2012).

Porém o dado mais interessante é a lei da oferta e demanda trabalhando em prol do crime. Existem cursos de treinamento de *carding* – roubo de credenciais de cartões de crédito – com três meses de duração na *deep web* brasileira. O curso ensina como criar *malware*, configurar *botnets* e hackear dados e credenciais de cartões de crédito, dentre outras invasões. No primeiro mês, os aprendizes são ensinados a invadir uma base de dados e furtar dados de cartão de crédito. Posteriormente, aprendem a etapa da compra feita com um cartão de crédito roubado quando é aprovada e como proceder caso falhe sua aprovação. No segundo mês, os alunos são ensinados como clonar cartões e a desenvolver cavalos de Tróia. Por R\$ 300, os aspirantes a cibercriminosos podem aprender a criar suas próprias espécies de *malware* e *phishing* (NORTON, 2012). Obviamente não é o sistema de mercado, denominado Capitalismo, o culpado pelo uso de suas logísticas para atos ilícitos, porém, não obstante, deve haver a reparação para que estes atos ilícitos não ocorram.

O governo brasileiro precisa investir mais recursos nas investigações já que os ataques de integridade são inéditos, mais sofisticados, bem planejados e executados. A alteração, discretamente, de transações ou de dados específicos pode gerar danos mais severos, gerando lucros astronômicos para o crime organizado atuante na *web*. Pesquisadores detectaram o *Carbanak*, ataques a bancos que modificava um número pequeno de específicas operações, roubando entre US\$ 300 milhões e 1 bilhão de mais de 100 bancos. Atividades maliciosas têm surgido em departamentos com e-mails de *phishing* com solicitações para enviar cheques a fornecedores estrangeiros, sendo transações completamente fraudulentas (NORTON, 2012). O relatório de ameaças do McAfee Labs (2015) divulgou que no terceiro trimestre de 2015 a empresa já havia detectado mais de 5 milhões de amostras de *ransomware*. O *CryptoWall*, um popular *ransomware*, conseguiu mais de US\$ 320 milhões no ano passado a partir de vítimas que pagaram a extorsão. Consumidores, empresas e agências governamentais pagaram para ter seu acesso aos dados restaurado. A escala de *ransomware* nunca foi tão grande e continua a crescer, alimentada por seu próprio sucesso. Os criminosos se beneficiam das vantagens deste tipo de ataque e seguirão por tanto tempo quanto puderem.

Enquanto a maioria das pessoas associa extorsão a filmes de Hollywood e mafiosos, os cibercriminosos usaram o *ransomware* para transformar a extorsão em uma empresa lucrativa,

atacando alvos grandes e pequenos. O *cryptoransomware* mantém os arquivos de uma vítima, as fotos e outros meios digitais como reféns sem mascarar a intenção do atacante. A vítima recebe uma chave para descriptografar seus arquivos, mas só depois de pagar um resgate que pode variar de US\$ 300 a 500 e isso ainda não garante que seus arquivos serão liberados ou não divulgados. No nível humano, o *ransomware* é uma das formas mais desagradáveis de ataque para as vítimas. Os criminosos usam *malware* para criptografar os dados dos discos rígidos das vítimas e exigem pagamento para desbloquear os arquivos. A melhor, e basicamente a única, defesa é manter um backup separado de seus arquivos, de preferência *offline*, para restaurar a partir da mesma. Há muitas variantes de resgate e nenhum sistema operacional garante imunidade. Embora o conselho permaneça o mesmo – não pague os criminosos – muitas empresas e indivíduos simplesmente querem ou precisam de seus arquivos de volta. Então eles pagam e assim o *scam* permanece rentável. Para pagar o resgate, a vítima tem que visitar uma página na rede *Tor*, na *dark web* e o pagamento é então solicitado em *bitcoins*. Estes são movimentos típicos de um criminoso *cryptoransomware*, tornando incrivelmente difícil rastrear e encerrar tais golpes (MCAFEE LABS, 2015).

O lucro é o ponto crucial de todo *scam*. A Symantec estimou que os cibercriminosos que estavam por trás do *CryptoDefense* ganharam mais de US\$ 34 mil em apenas um mês, com pesquisadores descobrindo que fez mais de US\$ 1 milhão em um período de seis meses. Não é de admirar que o *cryptoransomware* seja considerado a operação de cibercrime mais eficaz no momento (MCAFEE LABS, 2015). Como consequência dessa dinâmica, cresce o volume de ações consideradas mais simples, como o *phishing*, que aposta na ingenuidade dos internautas para fazer as suas vítimas. Esse ataque consiste em enviar e-mails e mensagens de texto em massa, com arquivos maliciosos ou links para páginas falsas, que simulam as de empresas legítimas. Internautas desavisados então informam seus dados pessoais, até mesmo bancários, que vão parar nas mãos de criminosos. Já o chamado Kit Boleto é mais sofisticado e aproveita uma forma de pagamento exclusiva do Brasil. Os hackers exploram táticas, inclusive o *phishing*, para instalar um software na máquina da vítima. Quando o consumidor gera um boleto pela internet, o programa altera o código de barras, direcionando o pagamento para uma conta bancária sob seu controle. A maior parte das operações realizadas pela PF é justamente relacionada a fraudes bancárias, muitas vezes *phishing* (MATSUURA; JANSEN, 2015).

A operação Sheik é um exemplo de sucesso no combate a esse tipo de crime e mostra o tamanho do prejuízo causado apenas com computadores. Três pessoas foram detidas em Uruaçu e Goiânia pois acessavam pela internet 4.032 contas bancárias, movimentando indevidamente cerca de R\$ 2 milhões de reais. A PF participou, em parceria com o FBI e a Europol, de outra

operação, a Darkode, que resultou na prisão de outros dois hackers em Goiânia e Belo Horizonte, acusados de terem movimentado mais de R\$ 1 milhão de reais pela venda de dados bancários roubados. Realizada simultaneamente em diversos países, a operação prendeu cerca de 70 cibercriminosos e tirou do ar um fórum digital mantido pelos hackers (MATSUURA; JANSEN, 2015).

Ou seja, o mesmo sistema de mercado, o qual adapta-se às necessidades e faz com que empresas se adaptem – ou, pelo menos, tentem –, funciona para que os cibercriminosos também se adaptem de forma organizada e comercial a ponto de haver fóruns e leilões de itens/dados obtidos ilicitamente, cursos preparatórios para hackers e criação de conjuntos de hackers para ataques orientados. É a lei da oferta e demanda funcionando para os criminosos, de tal maneira que discursos como “devemos ir a pequenos passos” ou “devemos tomar cuidado com discursos contraterrorismo” somente ajudam a imensa maioria a se esquivar de suas devidas sanções e viver neste mundo de fácil anonimato e sem praticamente nenhum mecanismo para a resolução destes problemas. De acordo com dados do Wüest (2015), Trendmicro (2015) e Secureworks (2016), temos a seguinte tabela no mercado negro na *deep web*, onde os preços podem variar dependendo do vendedor e de sua respectiva credibilidade (Tabela 01):

Tabela 01 – Tabela de preço de dados na *deep web*.

| ITEM                                 | CUSTO (US\$) | USOS                              |
|--------------------------------------|--------------|-----------------------------------|
| 1.000 contas de e-mail roubadas      | 0.5 a 10     | <i>Spam, phishing</i>             |
| Detalhes do cartão de crédito        | 0.5 a 20     | Compras fraudulentas              |
| Scanner de passaportes reais         | 1 a 2        | Falsificação de identidade        |
| Contas de jogos roubadas             | 10 a 15      | Ganhar itens de valor virtual     |
| <b>Malware customizado</b>           | 12 a 3.500   | Pagamentos diversos               |
| 1.000 seguidores em redes sociais    | 2 a 12       | Gerar interesse com visualizações |
| <b>Roubo de contas em cloud</b>      | 7 a 8        | Obter um Server de C&C            |
| <b>1 milhão de spams a e-mails</b>   | 70 a 150     | <i>Spam, phishing</i>             |
| <b>Credenciais de contas de apps</b> | 155 a 193    | Fraude                            |
| Credenciais de cartões de créditos   | 35 a 155     | Compras fraudulentas              |
| Credenciais de contas de serviços    | 19           | Fraude                            |
| Lista de números de celulares        | 290 a 1.236  | Fraude e falsificação ideológica  |

|                                                        |               |                                      |
|--------------------------------------------------------|---------------|--------------------------------------|
| Lista de números de telefone fixo                      | 317 a 1.931   | Fraude e falsificação ideológica     |
| <i>Social Security Number</i>                          | 30            | Falsificação ideológica              |
| Data de Nascimento                                     | 11            | Falsificação ideológica              |
| Credenciais do Seguro de Vida                          | 7             | Fraude                               |
| 300 endereços IP                                       | 6             | <i>Hacking</i>                       |
| Conta de banco com<br>US\$ 70.000,00 a US\$ 150.000,00 | 300 ou menos  | Pagamentos diversos                  |
| <b><i>“Kitz” de todas informações</i></b>              | 1.200 a 1.300 | Fraude, falsidade ideológica<br>etc. |

(Fonte: WÜEST, 2015; TRENDMICRO, 2015; e SECUREWORKS, 2016)

## CAPÍTULO 2 ESTADO, DIREITO E INTERNET

### 2.1 IMPRESCINDIBILIDADE ESTATAL

*Não basta justificar a existência e necessidade do Estado por normas jurídicas propostas por este mesmo Estado.*

Matteucci nota alguns empecilhos na definição do Estado Contemporâneo:

Uma definição de Estado contemporâneo envolve numerosos problemas, derivados principalmente da dificuldade de analisar exaustivamente as múltiplas relações que se criaram entre o Estado e o complexo social e de captar, depois, os seus efeitos sobre a racionalidade interna do sistema político. Uma abordagem que se revela particularmente útil na investigação referente aos problemas subjacentes ao desenvolvimento do Estado contemporâneo é a da análise da difícil coexistência das formas do Estado de direito com os conteúdos do Estado social. Os direitos fundamentais representam a tradicional tutela das liberdades burguesas: liberdade pessoal, política e econômica. Constituem um dique contra a intervenção do Estado. Pelo contrário, os direitos sociais representam direitos de participação no poder político e na distribuição da riqueza social produzida. (MATTEUCCI, 1998, p. 401).

A estrutura do Estado de Direito hodierno pode ser sistematizada em quatro partes: 1) Estrutura formal do sistema jurídico de garantia das liberdades fundamentais com a aplicação da lei geral-abstrata por juízes independentes; 2) Estrutura material do sistema jurídico para liberdade de concorrência no mercado; 3) Estrutura social do sistema jurídico para a questão social e políticas reformistas de integração da classe trabalhadora; e 4) Estrutura política do sistema jurídico de separação e distribuição do poder (NEUMANN, 1973). Em todo caso, o Estado cumpre o papel de consolidador dos direitos básicos da sociedade.

E para a análise destas estruturas, vamos utilizar algumas premissas contratualistas, especialmente de Hobbes, mesmo tendo o Contratualismo encontrado dois problemas: a hipótese da origem, do estado de natureza através de um contrato que se revelou totalmente abstrata após estudos antropológicos, e o oferecimento de escassas possibilidades teóricas a quem quisesse apenas explicar a ordem orgânica e a mudança social devida dos conflitos. O Contratualismo é, acima de tudo, uma teoria prescritiva acerca da melhor ordem política e tem ocupado recentemente um lugar central no campo da filosofia política: partindo do pacto social, ou seja, das regras que têm de ser estabelecidas antes do seu início, procura-se encontrar um fundamento para a obrigação política e o cumprimento da lei.

Sendo justamente neste momento que se pode encontrar, na pontuação de políticas públicas e normas adequadas, problemas sobre a legitimidade e imprescindibilidade estatal e,

neste caso, no seu tratamento com a internet. Hobbes teve interessantes insights acerca da natureza humana e da sua necessidade de se autocontrolar através de um ente com poder concentrado. Apesar de fundador de doutrinas absolutistas e de ser um Contratualista, eis algumas suas interessantes descrições:

O fim último, causa final e desígnio dos homens (que amam naturalmente a liberdade e o domínio sobre os outros), ao introduzir aquela restrição sobre si mesmos sob a qual os vemos viver nos Estados, é o cuidado com sua própria conservação e com uma vida mais satisfeita. Quer dizer, o desejo de sair daquela mísera condição de guerra que é a consequência necessária (conforme se mostrou) das paixões naturais dos homens, quando não há um poder visível capaz de os manter em respeito, forçando-os, por medo do castigo, ao cumprimento de seus pactos e ao respeito àquelas leis de natureza que foram expostas nos capítulos décimo quarto e décimo quinto. Porque as leis de natureza (como a justiça, a equidade, a modéstia, a piedade, ou, em resumo, fazer aos outros o que queremos que nos façam) por si mesmas, na ausência do temor de algum poder capaz de levá-las a ser respeitadas, são contrárias a nossas paixões naturais, as quais nos fazem tender para a parcialidade, o orgulho, a vingança e coisas semelhantes. E os pactos sem a espada não passam de palavras, sem força para dar qualquer segurança a ninguém. Portanto, apesar das leis de natureza (que cada um respeita quando tem vontade de respeitá-las e quando pode fazê-lo com segurança), se não for instituído um poder suficientemente grande para nossa segurança, cada um confiará, e poderá legitimamente confiar, apenas em sua própria força e capacidade, como proteção contra todos os outros. (HOBBS, 2003, p. 59).

É tentador pensar na natureza animal humana como uma irracionalidade sempre presente e maléfica para o convívio social de bem-estar. Hobbes cita seis motivos pelos quais o homem deve se organizar de forma social e conjunta com um ator com poder concentrado, diferente de outros animais. São elas: a) os homens estão constantemente envolvidos numa competição pela honra e pela dignidade, gerando inveja, ódio e guerra; b) o homem só encontra felicidade na comparação com os outros homens e só pode tirar prazer do que é eminente; c) os homens são em grande número os que se julgam mais sábios e mais capacitados que os outros para o exercício do poder público, acabando assim por levar o país à desordem e à guerra civil; d) cada homem tem sua concepção sobre o bem ou o mal, semeando o descontentamento entre os homens e perturbando a seu bel-prazer a paz em que os outros vivem; e) o homem é mais implicativo quanto mais satisfeito se sente, pois é neste caso que tende mais para exibir sua sabedoria e para controlar as ações dos que governam o Estado; e f) o acordo dos homens surge apenas através de um pacto, isto é, artificial e subjetivamente, é necessária alguma coisa mais, além de um pacto, para tornar constante e duradouro seu acordo: ou seja, um poder comum que promova respeito e atue pelo benefício comum (HOBBS, 2003, p. 61). Assim, perante a necessidade de um Estado, a única maneira de instituir um tal poder comum garantindo-lhes uma segurança suficiente, mediante seu próprio labor e que graças aos frutos da terra possam alimentar-se e viver satisfeitos, é conferindo toda sua força e poder a um homem ou a uma assembleia de homens, diluindo suas diversas vontades, por pluralidade de votos, a uma só

vontade, para a paz e segurança comuns. Feito isto, a multidão unida numa só pessoa se chama Estado, dos *civitas* (HOBBS, 2003, p. 61).

Dentro da sociedade, deseja-se encontrar um consenso entre a vontade geral e os interesses particulares, já que os homens, antes do salto para a sociedade, querem sua justiça, ou seja, maximizar suas posições mínimas. Assim, são delineados os dois princípios de justiça básicos de cada sociedade e Estado democrático: “cada indivíduo possui direito igual à mais ampla liberdade possível, compatível com a igual liberdade dos outros” e “as desigualdades sociais e econômicas não de ser estruturadas de modo que sejam razoavelmente geradoras de vantagens para todos e ligadas a posições e cargos igualmente abertos a todos” (MATTEUCCI, 1998, p. 283). Tais analogias transparecem ser arcaicas se não adaptadas à realidade complexa e avançada em que vivemos. Hoje os atos ilícitos são sempre relativos, havendo a necessidade de observar cada caso a esgotar as possibilidades concorrentes e observar todos os fatos incidentes e os que (não) influenciam no ato. A noção de que todos nós assinamos um teórico contrato é ultrapassada de fato e não é o ponto o qual discutimos. Na observância da existência de diversas espécies e razões dos atos ilícitos, para aqueles praticados no meio digital, é simples a analogia: existem milhões de atos ilícitos sendo praticados por dia na internet cuja imensa maioria não é solucionada ou passível de indenização, logo, deve alcançar o Estado a resolução destes problemas.

Porém, é neste momento que há de se separar a noção de Estado-árbitro – com monopólio da sanção e imposição do cumprimento do ordenamento – e o Estado produtivo – fornecedor dos bens públicos. Um Estado Mínimo teria a única função de proteger os direitos individuais contra qualquer forma de violação dos mesmos. Surgindo, assim, novos limites constitucionais mediante a atual crise do Estado Assistencial ou do bem-estar (MATTEUCCI, 1998, p. 401). Um dos problemas atuais desta legitimação do Estado é reconhecido por Luhmann (1979), que enxerga as dificuldades da legitimação por processo, visto que o procedimento administrativo cada vez menos produz efetivas diretrizes políticas: a política decide apenas as modalidades das decisões administrativas, mas não lhes determina os conteúdos. Havendo também a crise da teoria dos sistemas, já que é a política administrativa, adaptando-se passivamente em cada caso aos problemas, que deve renunciar o corpo social dentro de procedimentos formais. Cada vez mais o meio de comunicação encontra fontes de poder impossíveis de se controlar, estabelecendo um tipo de “politicismo localista baseado na especificidade de determinados minissistemas” (LUHMANN, 1979, p. 113, tradução nossa). Assim, a nova estrutura social exige núcleos cada vez mais descentralizados.

Por si só, as motivações expostas para a obediência às normas estatais não são autossuficientes, são somente explicativas. Talvez nunca serão justificadas, afinal, não basta justificar a existência e necessidade do Estado por normas jurídicas propostas por este mesmo Estado, através da Teoria do Direito. A justificativa somente pode se dar pela prática, pelos (bons) resultados de sua existência e pelas consequências de seus atos. Entrando aí as consequências observadas, por liberais ou estatistas, com seus pontos de vistas sobre causas e consequências sobre um mesmo evento social a ser ou não desregulamentado pelo Estado. As funções do aparelho político representativo não desempenham mais só a tarefa de garantir a lealdade de massa, mas também a de tutela da segurança nacional (MATTEUCCI, 1998, p. 401). Principalmente na anárquica internet, onde somente com as diretrizes constitucionais pode-se definir melhores soluções para os problemas encontrados na mesma. Em um futuro ainda distante, o ideal seria a organização de ordens jurídicas globais e plurais (*law's global villages*), organizadas estruturalmente com um dos sistemas mundiais, como a internet, através de Constituições civis (NEVES, 2009, p. 113), como ainda veremos.

## 2.2 DIREITO DIGITAL

*Um direito rígido não terá uma aplicação eficaz.*

Muito se fala sobre internet e a falta de segurança na proteção dos dados pessoais dos usuários, mas pouco se tem feito para ativamente coibir as violações. Segundo Leonardi (2009, p. 40), as principais correntes as quais idealizam as formas mais eficazes de regulamentação da internet são: a) autorregulação, mediante regras e princípios estabelecidos pelos próprios usuários do ciberespaço; b) criação de um “direito do ciberespaço” separado do direito convencional, com apoio em tratados e convenções internacionais; c) aplicação dos institutos jurídicos tradicionais, com o emprego da analogia para lidar com a internet; e d) abordagem mista, utilizando o sistema jurídico em conjunto com a própria arquitetura dessa rede. Dentre as várias teorias da criação de uma regulação da internet, que pelas consequências das características singulares da rede não demonstraram ter muita eficácia, a teoria de abordagem mista parece ser uma exceção.

A princípio, todos esses termos estão correlacionados: Direito Informático, Direito da Informática, Cyberlaw, Direitos Virtuais, Direito Cibernético, Direito da Internet, Direito Eletrônico, Direito Digital, e-Law etc. Certo é que o termo que “pegou” foi Direito Digital e

que, portanto, usaremos. Por exemplo, a expressão genérica Crime Cibernético diz respeito a série de crimes que se pode praticar com o uso do meio digital. Podemos incluir nele: plágio; pirataria; ameaça; difamações; calúnias; injúria; racismo; discriminação; preconceito; pedofilia; pornografia ilegal; ataques virtuais; vírus; golpes; falsa identidade; *phishing* (quando informações particulares ou sigilosas, como CPF ou senha de acesso são hackeadas); uso indevido de senha; vazamento de informação confidencial; furto de dados; concorrência desleal; uso não autorizado da marca na internet; fraudes; chantagem; falsificação; apropriação indébita; estelionato; invasão de privacidade, em geral; dentre tantas outras formas de usar o meio digital ilicitamente.

Um dos principais problemas na regulamentação da internet é o seu alcance global, afinal, não é possível observar a rede de forma restrita. No entanto, os órgãos estatais limitam-se a estabelecer diretrizes para um desenvolvimento ético e funcional da rede. Sem a real coercibilidade de normas e ferramentas combatentes do cibercrime, não há um controle eficaz do uso da internet. Afinal, sem a potencial aplicação de sanções, não é possível vincular as condutas dos indivíduos visando a diminuição de práticas lesivas pela rede.

Outro problema é o conhecimento técnico que esta área jurídica exige. Juristas, sejam eles as partes ou os magistrados, precisam adaptar-se à linguagem e metodologias. Em um caso emblemático no STJ, sobre a indenização sobre *spams* que preconizou a responsabilidade do ofertante por abuso do direito sem prejuízo das sanções da publicidade abusiva e o Presidente da turma julgadora, Min. Fernando Gonçalves, disse que “não sei nada de computador e nem quero saber”, mostrando-nos a gravidade do problema. Vejamos a jurisprudência:

Danos Morais. *Spam*. Trata-se de ação de obrigação de fazer cumulada com pedido de indenização por danos morais em que o autor alega receber e-mails (spam com mulheres de biquíni) de restaurante que tem show de streaptease e, mesmo tendo solicitado, por duas vezes, que seu endereço eletrônico fosse retirado da lista de e-mail do réu (recorrido), eles continuaram a ser enviados. Entre os usuários de Internet, é denominada spam ou spammers mensagem eletrônica comercial com propaganda não solicitada de fornecedor de produto ou serviço. A sentença julgou procedente o pedido e deferiu tutela antecipada para que o restaurante se abstinhasse do envio da propaganda comercial sob pena de multa diária, condenando-o a pagar, a título de danos morais, o valor de R\$ 5 mil corrigidos pelo IPC a partir da data do julgamento, acrescidos de juros de mora, contados a partir do evento lesivo. Entretanto, o TJ proveu apelação do estabelecimento e reformou a sentença, considerando que o simples envio de e-mails não solicitados, ainda que dotados de conotação comercial, não configuraria propaganda enganosa ou abusiva para incidir o Código de Defesa do Consumidor (LGL\1990\40) e não haveria dano moral a ressarcir, porquanto não demonstrada a violação da intimidade, da vida privada, da honra e da imagem. Para o Ministro relator, que ficou vencido, o envio de mensagens com propaganda, quando não autorizada expressamente pelo consumidor, constitui atividade nociva que pode, além de outras consequências, gerar um colapso no próprio sistema de Internet, tendo em vista um grande número de informações transmitidas na rede, além de que o spam teria um custo elevado para sociedade. Observou que não há legislação específica para o caso de abusos, embora existam projetos de lei em tramitação no Congresso. Daí se aplicar por analogia o CDC (LGL\1990\40). Após várias reflexões sobre o tema,

reconheceu a ocorrência do dano e a obrigação de o restaurante retirar o autor de sua lista de envio de propaganda, e a invasão à privacidade do autor, por isso restabeleceu a sentença. **Para a tese vencedora, inaugurada pelo Min. Honildo de Mello Castro, não há o dever de indenizar, porque existem meios de o remetente bloquear o spam indesejado, aliados às ferramentas disponibilizadas pelos serviços de e-mail da Internet e softwares específicos, assim manteve a decisão do Tribunal a quo.** Diante do exposto, a Turma por maioria não conheceu do recurso. (BRASIL, 2009, grifo nosso).

Todas as vezes que algo novo surgir na sociedade ter-se-á que criar um ramo novo do Direito para regrá-lo? A internet de fato é um novo meio para a realização de velhos delitos, os crimes relativos, contando com sua possível eficácia por um curtíssimo período temporal. Todavia, o ordenamento jurídico pré-existente não consegue lidar com os outros crimes, os puros. E secundamente, pela extensão da rede e, principalmente, pelos milhões de atos ilícitos a serem tutelados, diferente de outros casos, e por uma insuficiência da sociedade e do meio privado, temos a necessidade deste novo Direito Digital. Uma analogia pode ser feita com a lei prussiana de ferrovias de 1838 quando gerou o dever de ressarcir baseado no risco da atividade (PONTES DE MIRANDA, 2012, p. 56). Assim, ela não foi simplesmente uma adaptação interna do mercado da época, mas uma lei sobre a organização pública da atividade econômica em âmbito nacional assim como leis em âmbito de Direito Digital o são, como o MCI e a LGPD.

Diante disso, as normas legais que tratam da internet não devem ser casuísticas e, sim, ter caráter aberto para a garantia de sua permanência e longevidade, já que aspectos com demasiadas especificidades tornar-se-ão obsoletos em pouco tempo. É de mister importância a busca de coibições, através da criação de órgão fiscalizador como a ANPD, para a captura de cibercriminosos, que difere e muito das possibilidades que o Direito Penal por exemplo tutela. Buscando-se, dessa forma, a criação de um Direito Digital não apenas preocupado necessariamente com crimes os quais a internet só seja um veículo, os crimes relativos, mas sim preocupando-se com medidas de combate a todas espécies de ciberataques e com a solução à vulnerabilidade e à ineficácia generalizada do meio privado.

Diversos países, como a Inglaterra e os Estados Unidos, já possuem em suas Faculdades de Direito, centros de estudos sobre normas jurídicas e internet, e oferecem, também, a disciplina *Cyberlaw* em seus cursos. No Brasil, já se observa os primeiros passos ao ministrarem, em algumas faculdades de direito, disciplinas e grupos de estudo que envolvem esse novo tema sobre internet e sua relação com o Direito e já existem também cursos de pós-graduação destinados a este tema. O MEC aprovou a Resolução n. 5/2018, que incluiu as disciplinas de Direito Digital e Direito Financeiro na grade curricular das faculdades. Lembrando que na Resolução n. 2/2021 do MEC, que também incluiu no PCC (Prática como

Componente Curricular) conteúdos essenciais referentes às áreas de Direito, houve uma mistura dos termos Direito Digital e Direito Cibernético, mas nada que atrapalha a consolidação da disciplina. Porém, tanto no Brasil como em outros países, a principal dificuldade está em encontrar soluções eficientes diante da realidade cibernética.

Leonardi (2005, p. 170) fala do modelo geral de regulação de Lawrence Lessig (1999), o qual se subdivide em quatro modalidades de regulação: o direito, as normas sociais, o mercado e a arquitetura. Analisando essas modalidades de regulação, temos que: a) o direito nem sempre é a maneira mais eficiente para a satisfação da cibervítima; b) as normas sociais regulam o comportamento na rede sem regras estabelecidas; c) o mercado regula também o comportamento na rede por meio da cobrança dos serviços prestados; e d) a modificação da arquitetura original da internet busca a proteção de determinado direito. Essas quatro modalidades de regulação interagem entre si, tornando, teoricamente, o direito imutável mesmo mediante a hiperdinâmica da rede. Porém, o caso de atos ilícitos praticados através de meios digitais já devidamente tutelados por outras leis não é o intuito na defesa deste trabalho e sim a criação de um Direito Digital voltado à resolução de problemas jurisdicionais, à diminuição destes crimes e à captura de cibercriminosos.

A lei deve ser instrumento capaz de garantir e gerir os direitos fundamentais estabelecidos na Constituição Federal, refletindo seus valores. Devem nortear essas relações cibernéticas a dignidade da pessoa humana, a transparência, a boa-fé, o equilíbrio, a privacidade, a segurança, a proteção dos interesses econômicos e dos direitos do consumidor, para que seja estabelecida a confiança entre os entes do meio digital. Para Patrícia Peck Pinheiro, o Direito Digital não é algo novo, mas sim um produto derivado da legislação atual, como qualquer lei extravagante:

Não devemos achar, portanto, que o Direito Digital é totalmente novo. Ao contrário, tem ele sua guarida na maioria dos princípios do Direito atual, além de aproveitar a maior parte da legislação em vigor. A mudança está na postura de quem a interpreta e faz sua aplicação. [...] O Direito tem de partir do pressuposto de que já vivemos uma sociedade globalizada. Seu grande desafio é ter perfeita adequação em diferentes culturas, sendo necessário, por isso, criar a flexibilidade de raciocínio, nunca as amarras de uma legislação codificada que pode ficar obsoleta rapidamente. (PINHEIRO, 2009, p. 35).

Por fim é válido salientar que, nesta Era Digital, o instrumento de poder é a informação. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso à informação. Portanto, o Direito é a somatória de comportamento e linguagem e, hoje, esses dois elementos estão mais flexíveis e dinâmicos do que nunca, demonstrando que um direito rígido não terá uma aplicação eficaz.

Há debates acadêmicos sobre o Direito Digital ser uma disciplina autônoma, juntamente a tantas outras que ainda busca este clássico status positivista, como o Direito Desportivo, o Direito Filosofia do Direito, Introdução ao Estudo do Direito e História do Direito, Biodireito (muitas vezes sinônimo de Direito Médico), Direito Comparado, Direito Econômico (muitas vezes sinônimo de Direito Financeiro), Direito Militar, dentre outras. Poder-se-ia argumentar que, por exemplo, a Introdução ao Estudo do Direito é matéria que não cria saber, apenas recolhe informações de outras disciplinas jurídicas para compor seu conhecimento. Mesmo assim, ela desempenha função exclusiva, que não se confunde com a de qualquer outra e sua autonomia deriva de seu fim específico de reduzir o Direito uma unidade sistemática. Assim também é autônomo o Direito Digital, que mais ainda, produz conhecimento fora das tradicionais disciplinas, além de, claro, complementá-las. O Direito Digital precisa ser ensinado separadamente, pois recorrentemente docentes das disciplinas tradicionais sequer mencionam a internet. Por exemplo, hoje o consumo de mercadorias é realizado em enorme parte, quem sabe a maioria, no meio digital. E como poderia um professor de Direito do Consumidor não saber as diversas nuances e diferenças deste meio com o meio real? Tal lógica também se aplica ao Direito Civil (com contratos eletrônicos, herança digital etc.) e ao Direito Penal (com invasão de dispositivo informático, divulgação de imagem íntima etc.). Assim, o Direito Digital requer uma formação universitária específica ou com um indexador próprio em bancos de dados bibliográficos. No extremo caso da academia jurídica desconsiderar sua autonomia, não haveria obstáculo que o Direito Digital que este já não sofre e desbrava no ensino jurídico. Vejamos que alguns de embasamentos conceituais são importados das disciplinas jurídicas fundamentais tradicionais, porém a maioria de seus conceitos são exclusivamente criados para ele, pois se distancia e separa destas tanto pelo objeto específico (objetividade própria) de seu estudo como pela metodologia própria que o caracteriza, sem prejuízo de sua perspectiva interdisciplinar e multidisciplinar. Se a autonomia de um ramo do direito verifica-se com a existência de normas e princípios específicos dentro de um ordenamento jurídico, o Direito Digital tem, portanto, autonomia. A consolidação do Direito Digital como disciplina autônoma, auxiliaria ainda mais na organização de seus métodos e teorias, valores, princípios e fontes, já que um novo ramo do direito pode se desenvolver resguardando o método dialógico e interdisciplinar. Logo, o Direito Digital forma um ramo novo da ciência jurídica, pois tem objetivos, conclusões, finalidades e resultados que não são de nenhuma outra disciplina jurídica.

No contexto internacional, o Estado não desaparece, é apenas redimensionado na Era da Informação com regiões negociando com governos nacionais, empresas multinacionais e órgãos internacionais. O que os governos locais e regionais não têm em termos de poder e

recursos é compensado pela flexibilidade e atuação em redes (CASTELLS, 2007, p. 259). Mundialmente, o principal e talvez o único instrumento jurídico significativo o qual possui regras gerais e específicas para tutelar cibercrimes é a Convenção de Budapeste, de 2001, com normas majoritariamente de Direito Penal Material. O principal destaque da Convenção é que define: os cibercrimes (Capítulo I), tipificando-os como infrações contra sistemas e dados informáticos (Capítulo II, Título 1); infrações relacionadas com computadores (Capítulo II, Título 2); infrações relacionadas com o conteúdo, como a pornografia infantil (Capítulo II, Título 3); e, também, infrações relacionadas com a violação de direitos autorais (Capítulo II, Título 4). Jurisdição e integração internacional são vistas no seu artigo 22, o qual aponta quando e como uma infração é cometida, além de recomendar aos seus aderidos a “jurisdição mais apropriada para o procedimento legal” (BRASIL, 2001, p. 14-15).

Mediante à flexibilidade da Convenção, questiona-se: por que o Brasil não adere às diretrizes da Convenção de Budapeste? Como não fora um dos signatários originais do tratado, o Brasil não pode simplesmente aderir à Convenção e sim, ser convidado pelo Comitê de Ministros do Conselho Europeu (BRASIL, 2001, p. 14-15). Até o presente momento desta dissertação, a adesão do Brasil à Convenção foi aprovada pelo Senado, cujo Projeto de Decreto Legislativo 255/2021 aguarda promulgação pelo Congresso Nacional.

O debate internacional e nacional sobre uma tutela global de cibercrimes é bastante polarizado. Alguns países da Convenção de Budapeste entendem a necessidade de universalizar o sistema jurídico que tutela dos cibercrimes e existem outros países, como o Brasil, China, Índia e Rússia, que já pretendem negociar um acordo universal, independente da Convenção de Budapeste. Sendo assim, essas duas visões distintas sobre o combate ao cibercrime tornam o processo de avaliação de um instrumento universal vagaroso. Ou seja, existe um vazio internacional para combater crimes cibernéticos (CPI – CRIMES CIBERNÉTICOS, 2016, p. 6-7). Não há como cogitar soluções eficazes e, ao mesmo tempo, nacionais para muitos destes crimes, devendo o assunto ser debatido em âmbito internacional. Os objetivos desta Convenção restaram claramente demonstrados, considerando a necessidade da previsão legal de tipos penais específicos, além do incremento da cooperação internacional, fundada na universalização de delitos perante os reflexos internacionais destes tipos. As barreiras encontradas pelos operadores do direito brasileiro no combate e na prevenção aos crimes digitais serão superadas com maior agilidade com a colaboração dos países signatários, além da otimização de seus procedimentos jurisdicionais.

É missão desse novo ramo jurídico adaptar institutos tradicionais às novas conquistas eletrônicas. Afinal, a lei é reativa, ela combate ou permite. E não há meio termo quando se lida

com a internet, pois tudo que é permitido é amplamente realizado na rede. O futuro breve definirá a autonomia desse novo ramo jurídico, por ter princípios, conceitos e legislações próprias. Enquanto não houver uma legislação específica para um novo crime, cabe ao jurista enfrentar os novos problemas com o Código Civil e legislação complementar (VENOSA, 2006, p. 263). Como observamos, alguns cibercrimes utilizam-se de técnicas um pouco distintas, pelas particularidades da internet e do meio digital, dos delitos tutelados pelo ordenamento penal brasileiro, mas o fim que se pretende é o mesmo da conduta já tipificada.

E é neste contexto que surge o Marco Civil da Internet, a Lei n. 12.965 de 23 de abril de 2014. É a principal lei que trata o uso da internet no Brasil, por meio de princípios e garantias, direitos e deveres para quem usa a rede, bem como algumas diretrizes para a atuação do Estado brasileiro. Porém, o seu maior enfoque foi com os provedores de serviços da internet e suas responsabilidades. O texto da lei trata de temas como neutralidade da rede, privacidade, retenção de dados, a função social da rede, a garantia da liberdade de expressão e da transmissão de conhecimento, além da responsabilidade civil aos usuários e provedores de serviços. Também trata, através do *caput* do art. 17, da obtenção de dados pessoais pelo Estado, referentes aos registros de conexões e de acesso de provedores de internet, condicionada a uma prévia decisão judicial devidamente fundamentada, já que estes dados podem compor um conjunto probatório em ações civis ou penais, em caráter incidental ou autônomo. Estando aí o Princípio da Reserva Jurisdicional. Um dos assuntos mais importantes são as aparições de decisões judiciais condenando os provedores por seu conteúdo publicado pelos usuários da rede, por ação ou omissão. Os provedores de conteúdo alegam que não dispõem de meios técnicos e humanos para fiscalizarem previamente todo o ambiente real-virtual. Afinal, há uma responsabilidade dos provedores de conteúdo, na omissão ou ação, e também na proteção e guarda de dados. Havendo aí outro problema prático a se resolver pelo ordenamento jurídico: até onde deve-se obrigar o provedor – e, portanto, sobrecarregá-lo pouco a pouco – para a proteção do usuário, de tal maneira a evitar o mínimo possível o prejuízo financeiro e profissional das empresas provedoras? Várias instituições de destaque apoiaram a aprovação do MCI, além de notórios documentos coletivos defendendo o projeto.

Na prática, por exemplo, há processos envolvendo Facebook, UOL, Google, WhatsApp e operadoras de telecomunicação com pedidos de remoção de conteúdo, de perfis e páginas falsas, indenização por envio de spam e pagamento de indenização por fraudes em compras na *web*. E mesmo com o Marco Civil, não existe uma legislação que abarque a totalidade dos crimes cibernéticos de maneira a resolvê-los por políticas públicas mínimas e auxiliar a força

policial na resolução dos milhares de atos ilícitos no meio digital, sendo estes muitas vezes tutelados de forma difusa em meio a tantas normas aplicáveis.

Outra lei importante é a Lei Geral de Proteção de Dados Pessoais (LGPD) cujo alvo principal é bastante parecido com o MCI: os provedores da internet (apesar de também se aplicar a particulares e entes federativos). Nesta lei, preocupa-se com os dados pessoais, sua coleta, consentimento, guarda e distribuição. Mas, apesar de introduzir a ANPD e o DPO, ainda não apresentou efeitos práticos ao combate dos extensivos abusos e *data breaches*.

O Direito Penal também vem sendo devidamente modificado para adaptar à realidade virtual, com a inclusão recente de institutos exclusivos do meio digital, como: Invasão de dispositivo informático (Art. 154-A), Furto qualificado mediante fraude cometido por dispositivo eletrônico (Art. 155, § 4º-B), Fraude eletrônica (Art. 171, § 2º-A), Registro não autorizado da intimidade sexual (Art. 216-B), Divulgação de cena de estupro, de sexo ou de pornografia (Art. 218-C), Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação (Art. 266). Vejamos que estas inclusões não excluem a importância do ensino autônomo do Direito Digital, pelo contrário, reforçam a necessidade de um estudo mais aprofundado destes temas.

Atualmente, podemos extrair os seguintes ordenamentos jurídicos aplicáveis que tratam do Direito Digital ou de algum dos tipos de cibercrimes, dentre outras são eles:

- Lei n. 12.965/2014: Marco Civil da Internet;
- Lei n. 13.709/2018: Lei Geral de Proteção de Dados Pessoais;
- Código Penal (Decreto-Lei n. 2.848/1940): crime de ameaça (art. 147); divulgação de segredo (art. 153); violação do segredo profissional (art. 154); invasão de dispositivo informático (Art. 154-A), este acrescentado pela Lei n. 12.737/2012, a Lei Carolina Dieckmann; furto qualificado mediante fraude cometido por dispositivo eletrônico (Art. 155, § 4º-B); extorsão (art. 158); fraude eletrônica (Art. 171, § 2º-A); violação de direito autoral (art. 184); registro não autorizado da intimidade sexual (Art. 216-B); favorecimento da prostituição (art. 228); interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação (Art. 266); incitação ao crime (art. 286); apologia de crime ou criminoso (art. 287); falsa identidade (art. 307); dentre outros.
- Lei n. 8.069/1990: pedofilia (art. 241);
- Lei n. 7.716/1989: crime de divulgação do nazismo (art. 20, §2º);
- Constituição Federal: art. 5º, incisos IV, V, X, XII e XIV;

- Código Civil (Lei n. 10.406/2002): arts. 186; 187; 205; 206; 212; 225; 927, parágrafo único; 932, inc. III; 1016; dentre outros.
- Código de Processo Civil (Lei n. 13.105/2015): arts. 332 e 333;
- Código de Processo Penal (Decreto-Lei n. 3.689/1941): arts. 156, 157 e 239;
- Lei n. 9296/1996 (Lei de Interceptação): arts. 1º, 3º, 9º e 10º;
- Consolidação das Leis Trabalhistas (CLT): arts. 482, incisos b, g, h;
- Lei n. 6.404/1976: arts. 153, 154, 155, 157, 158 e 159; etc.

## 2.3 CARACTERÍSTICAS JURÍDICAS DA INTERNET E DO MEIO DIGITAL

*As características jurídicas da internet têm enorme influência na organização normativa e regulamentadora da rede.*

Alguns doutrinadores consideram que os crimes praticados na internet são crimes comuns, não necessitando de novas definições. Outra corrente, a qual o presente trabalho se inclina por causa das características particulares da internet, representada por Luis Carlos Olivo (1998, p. 43), entende que “tais crimes devem ser divididos em crimes puros (aqueles que atingem um sistema, praticados por *hacker*, através de vírus) e crimes relativos (entendendo-se a internet como meio de execução da atividade delituosa)”. Percebe-se que os crimes cibernéticos têm características específicas, dependendo do bem jurídico tutelado e assim devem ser considerados ao se legislar e executar novas ferramentas jurídicas. Quanto aos crimes relativos, não há necessidade de uma nova tipificação por lei específica quando já existir predefinições, principalmente com o compilado de princípios e normas do Marco Civil da Internet, todavia, já os crimes puros requerem uma tipificação porque as leis atuais não as abrangem e muito menos solucionam.

Este subcapítulo preocupa-se com as características jurídicas da internet, as quais muitas vezes doutrinadores e leigos não se atentam e que têm enorme influência na organização normativa e regulamentadora da rede. Afinal, as consequências das características digitais são mais relevantes para nosso estudo do que as características em si. A mais clara delas é a virtualização (alguns a chamam de “natureza imaterial”), pois instrumentaliza a internet. Outra característica muito importante é a não rivalidade dos objetos virtuais, ou seja, que “não haverá a escassez da informação, pois a não rivalidade não excluirá do usuário o texto lido, a imagem

visualizada ou a música escutada”. Temos também a alta velocidade da circulação de informações (alguns a chamam de “instantaneidade do meio”), muito importante para a questão do direito ao esquecimento (MADALENA, 2016, p. 84). Também temos o altíssimo desconhecimento informático – devido à alta especialidade que a técnica demanda – dos usuários e até de empresas, como já constatado. Logo, quem tem este conhecimento, pode dele abusar sem reprimendas. Afinal, quanto mais individualizada – portanto, mais precisa – a informação de um usuário, mais os algoritmos poderão transformá-la em uma *commodity* altamente rentável (MADALENA, 2016, p. 84), neste caso na forma de dados sensíveis, e a quebra de segurança destes dados pode ser extremamente danosa. Outro ponto sobre esta característica é a impossibilidade prática de saber como seu dado é violado e qual a fonte de um suposto vazamento de certo dado. Como saber quais empresas e como as que possuem seus dados estão os guardando ou comercializando? Como saber qual a empresa que compartilhou primeiro certo dado? Por fim, a internet caracteriza-se pela sua deslocalização, devido à possibilidade de disponibilizar e de acessar informações que estejam armazenadas em servidores localizados em qualquer local do planeta, não importando o local físico da origem da informação.

Vejamos agora as consequências, de mister relevância para o Direito Digital, das características da internet e do meio digital.

### **2.3.1 Falsa Sensação de Anonimato e de Impunidade na Rede**

*O anonimato na rede torna cibercriminosos mais suscetíveis a praticar violações.*

A primeira e talvez a característica mais importante para que haja uma regulamentação estatal na internet é a conhecida dificuldade de identificação – e comprovação de quem está realmente atrás do teclado e do mouse – dos usuários. A internet, pelo altíssimo desconhecimento dos usuários e até de empresas especializadas, impossibilita em princípio que se saiba exatamente quem é o usuário, onde ele se encontra ou o que está fazendo, pois não há uma associação entre sua identidade, sua localização e seu comportamento pelo seu endereço IP (*Internet Protocol*). O mascaramento do IP é de fácil acesso através de aplicativos e programas explícitos em suas ações e até permitidas no mundo todo. Ou seja, há ínfimas possibilidades de identificação de preparados cibercriminosos, necessitando de investigações

longuíssimas da Polícia Federal para descobrir um ou dois atores dentre milhares no Brasil em períodos de meses e, não obstante, a PF ainda faz perícia da maioria dos casos que necessitam de algum tipo de comprovação ou prova digital, para milhares e diários casos no ordenamento jurídico. Empresas privadas raramente identificam o cibercriminoso e muito menos o denunciam ou sancionam. Hoje a ANPD apenas obriga a comunicação do *data breach*, mas não a identificação do cibercriminoso responsável. Como acrescenta Leonardi (2005, p. 157), “se não há uma maneira de saber quem alguém é, onde ele está, nem o que fez ou está fazendo, o sistema jurídico – que é dependente dessas informações para exercer sua força coercitiva – parece perder sua efetividade”.

Talvez o maior problema enfrentado na regulamentação da internet seja essa dificuldade de autenticação de um usuário específico, que se dá majoritariamente através do IP, ou seja, a dificuldade de se reconhecer automaticamente a identidade de quem está utilizando os serviços da rede mundial, ao inverso do que ocorre fora da internet, no mundo físico onde toda pessoa pode ser reconhecida pelo simples fato de ser vista por outra. Por isso, uma norma aplicada no mundo real pode não ter a mesma eficácia quando aplicada à internet. Sobre a carência de segurança e a facilidade de anonimato na rede, Pinheiro sugere que:

Uma prática recomendável seria obrigar os provedores a identificar suas contas ativas e inativas, utilizando uma tecnologia de fotografia do usuário, ou seja, ter a comprovação de seus dados e, se possível, uma imagem digital. Isso, associado a uma prática de cadastramento dos usuários, no mesmo procedimento adotado pelos bancos, permite que realmente existam meios de prova confiáveis, rompendo-se a maior barreira à segurança da rede. (PINHEIRO, 2009, p. 35).

E esta seria uma prudente medida. A exigência de RG, CPF e um e-mail de cadastro, o acréscimo de uma imagem digital e outros meios comprobatórios confiáveis poderiam ser ótimos meios para melhores identificações. Como supramencionado, um dos maiores entraves dos crimes virtuais é a raridade de denúncias e, pior, o despreparo – incluindo-se falta de pessoal e de recursos e não necessariamente uma falta de conhecimento – do meio privado em relação a cibercriminosos. São poucas as equipes de profissionais da polícia preparadas para a investigação do cibercrime. O estereótipo do cibercriminoso como alguém extremamente inteligente e habilidoso já não corresponde com a realidade. Estes cibercriminosos estão praticamente robotizados a sempre praticar uma ação que quase sempre dá certo e nunca é solucionada, como os golpes através de clonagem de números de WhatsApp através de anúncios da OLX. Assim, o anonimato na rede torna cibercriminosos mais suscetíveis a praticar violações da privacidade e da honra de outros indivíduos. Esta consequência psicológica de

pessoas cometerem maiores violações dos direitos alheios pela dificuldade de identificação do usuário foi denominada esquizofrenia cibernética.

O armazenamento de dados sobre as transações no meio digital ou sobre os protocolos IP são uma das melhores ferramentas de combate aos problemas de anonimato. Neste sentido, o Marco Civil acerta. Sua exigência de mudança de postura é necessária para que tenhamos uma sociedade digital segura; caso contrário, coloca-se em risco até o próprio Direito. O maior estímulo aos delitos virtuais é dado pela crença de que o meio digital é um ambiente marginal à realidade, um submundo em que a ilegalidade e a impunidade imperam. A sociedade não sente que este meio é suficientemente protegido e nem que podem eles ser punidos. Essa omissão de dispositivos garante uma sensação de anonimato e de impunidade, por ser na maioria das vezes regidas por entes privados, a quem, por má-fé, usa a internet para invadir propositalmente a privacidade de outra pessoa, tomando conhecimento, adulterando ou destruindo informações privadas e pessoais e, talvez a modalidade mais grave e permanente, divulgando tais materiais pela rede.

Há outros meios para obtenção e construção da identificação de cibercriminosos: a) Formulários: coleta de informações inseridas espontaneamente por usuários e se estes dados obtidos forem cruzados com outras PII (*Personally Identifiable Information*), poderá construir-se um perfil ainda mais completo; b) Cookies: pequenas informações captadas por sites visitados e armazenadas automaticamente no computador do usuário e no servidor do site visitado, como os navegadores utilizados, os horários acessados, o sistema operacional, as áreas de preferência e o número do IP, o que possibilita uma melhor identificação e localização física deste usuário; e c) Coleta de informações pelo Estado: regulamentação estatal somente em casos de suspeitas em que a averiguação de informações é útil para o desenvolvimento do perfil do cibercriminoso (SALES; LIMA; MIRANDA, 2016).

De qualquer maneira, há sempre alguma forma, dependendo do investigador, de identificar o infrator. Um exemplo foi a condenação de Ross Ulbricht à prisão perpétua, criador do maior *website* do mercado negro – o Silk Road – que intermediava traficantes de drogas, contrabandistas de pessoas e assassinos de aluguel a usuários na *deep web*. Demonstrando que, mesmo se praticados através de ferramentas que reduzem a identificação do usuário, estes infratores podem ser alcançados pelo Estado.

### **2.3.2 Eternalização de Condutas e Irreversibilidade do Dano**

*Na internet, as informações tornam-se eternas.*

A segunda característica é a eterna permanência da informação e sua consequente irreversibilidade do dano causado, pois uma vez inserida no mundo real-virtual lá permanecerá até que alguém a retire. Ela advém da alta velocidade da circulação de informações ou da instantaneidade do meio e se difere da informação produzida no mundo real pois neste último a notícia acaba por desaparecer com o decurso do tempo, visto que os meios materiais de reprodução (revistas, jornais, livros etc.) acabam por perder sua atualidade e são encontrados apenas em locais específicos e físicos para pesquisas. Na internet, devido à facilidade de busca e acesso da informação e à virtualidade do meio, as informações tornam-se eternas. Ou seja, há a tendência – com poucas exceções – de permanecer as violações aos direitos na internet, pois a qualquer tempo aquela informação poderá ser facilmente encontrada e redivulgada, diferentemente da busca de dados e informações passadas na realidade real que depende da pesquisa em bibliotecas, por exemplo. Sendo assim, a violação de direitos na rede deve ser tratada com maior severidade e rapidez.

Por isso falamos na eternização dos danos gerados por meio da internet, visto que hoje as pessoas são marcadas e julgadas regularmente por suas informações. Tais características podem gerar uma restrição à própria liberdade de expressão, pois os usuários, receosos das consequências eternas que a rede pode gerar, limitar-se-ão em sua comunicação na internet. Assim, diante de todos esses problemas apresentados, deve haver uma releitura do ordenamento jurídico criando-se critérios e regras específicas para disciplinar o tema. Afinal, apesar da primeira informação ter uma localização exata em certo servidor, após suas retransmissões e compartilhamentos, há uma deslocalização dos dados. Não se pode, com certeza, se retirar uma imagem ou dado sem a possibilidade de reincidência dela na própria internet. Outro ponto é que infrações na internet normalmente ocorrem em uma tal escala que torna impraticável para o titular fazer cumprir seus direitos contra cada infrator primário (ou que acessou e redivulgou o conteúdo que o atinge), quando já é difícil primeiramente identificá-los. Este é um dos motivos pelo qual é mais fácil para o titular do direito afetado entrar com ação contra a plataforma ou provedor, com a possibilidade de uma ação de regresso depois.

É através desta lógica que o presente trabalho buscará associar os atos ilícitos de crimes puros – não tão os crimes relativos os quais são facilmente tutelados por outras leis – com crime permanente, na tentativa de solucionar e estabelecer novas medidas aos problemas que enfrentamos.

A violação da honra e da privacidade no mundo virtual-real da internet apresenta consequências mais graves que tais violações no mundo real, podendo inclusive tornar-se irreversível na grande maioria das vezes, visto que as informações que circulam na rede ficam permanentemente gravadas e alcançam bilhões de pessoas que podem buscar tais informações a qualquer tempo com alta velocidade, exatidão e precisão. A irreversibilidade do dano advém da “não rivalidade dos objetos virtuais” já que a obtenção, uso ou exclusão de certo dado ou informação não exclui a possibilidade de outro fazê-lo com a mesma (ou cópia da) informação.

A amplitude destes atos praticados na internet tem potencial de alcançar todos seus usuários, bilhões de pessoas de qualquer todo o globo terrestre, levando a uma irreversibilidade dos atos ilícitos, devido à sua ubiquidade. Há alguns casos específicos de exceção, como por exemplo o uso inapropriado de marca satisfatoriamente resolvido pela remoção da empresa plagiadora, sem maiores prejuízos, exceto a potencial clientela e lucros perdidos que é subjetivamente calculado. Porém, nas redes sociais e nas atitudes ciberdelitivas, a irreversibilidade é facilmente identificável. Qualquer ato é registrado e mesmo que o conteúdo seja removido, vários usuários podem ter salvo a informação em algum hardware inacessível para a remoção deste conteúdo, permanecendo principalmente no servidor do provedor. O mais clássico exemplo são os recorrentes *porn revenge*, em que são tão somente esquecidos pela massa devido a instantaneidade de outros eventos ou plataformas. Todavia, os vídeos ficam ainda gravados em plataformas, mídias sociais, sites de pornografia e nos aparelhos dos usuários que recebem este tipo de dados. Ressalte-se, que esta irreversibilidade não impede um ressarcimento indenizatório e as tentativas por meios judiciais de retirar estes conteúdos da rede.

Essa particularidade torna extremamente perigosa a introdução dos atos ilícitos ou dos dados pessoais na internet, pois, após divulgada, a informação foge do controle de quem a publicou podendo ser reproduzida por milhares de outras pessoas. Por exemplo, uma notícia de interesse local publicada em um jornal local atingirá somente as pessoas daquela localidade e uma suposta violação aos direitos da privacidade deste jornal alcançaria um número limitado. Todavia, a mesma informação divulgada na internet poderá ter um alcance muitíssimo maior, a notícia poderá, assim, fugir do controle e ser reproduzida por milhares de pessoas atingindo um número de usuários inimaginável, ou seja, o dano causado pela violação da privacidade é imensuravelmente mais perigoso (GERALDINO, 2012, p. 11).

### 2.3.3 Superposição de Multiníveis de Responsabilidades dos Provedores

*A responsabilidade de um provedor variará de acordo com o serviço prestado.*

Para entender esta rede e suas particularidades, devemos nos atentar aos vários tipos de provedores, que são os prestadores de serviços na internet. São eles que fornecem ao usuário o acesso à internet, concedem a outros prestadores a plataforma necessária e garantem a armazenagem de mensagens e informações. As espécies de provedores se diferem de acordo com os tipos de serviços prestados, sendo eles os provedores de: *backbone*, acesso, hospedagem, conteúdo, informação, correio eletrônico, comércio eletrônico e de pesquisa. Os dois primeiros são provedores de conexão e os outros seis são provedores de aplicações. Tendo o fornecedor cumprido com seus deveres, em casos em que ocorre dano, deve-se verificar cada caso especificamente para decidir se existe ou não o dever de reparar, objetiva ou subjetivamente, devendo ser levado em consideração o art. 19 do Marco Civil da Internet:

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014).

O provedor de *backbone*, ou de “espinha dorsal”, representa o nível máximo de hierarquia de uma rede de computadores. É a ele que se ligam primordialmente os outros prestadores de serviços. Formado por múltiplos cabos de fibra óptica de alta velocidade, é o provedor que oferece a infraestrutura de cabos e pontos de acesso para que os outros provedores possam exercer suas atividades e oferecer seus serviços aos usuários. O provedor de *backbone* presta serviços ao provedor de acesso e ao provedor de hospedagem, que, por sua vez, agem como intermediários, podendo revender essa conectividade ao destinatário-consumidor final. Ele só será responsabilizado caso ocorra vícios na prestação de seus serviços ou equipamentos, respondendo pelos danos causados ao provedor de serviços ou até Estados que usam sua infraestrutura, na forma do art. 931 do CC (SÁVIO, 2013, p. 54). No Brasil, as empresas prestadoras deste serviço são: BrasilTelecom, Telecom Itália, Telefônica, Embratel, Global Crossing e a Rede Nacional de Ensino e Pesquisa (RNP).

O provedor de acesso já é a pessoa jurídica fornecedora de serviços que possibilitam o acesso de seus consumidores-usuários à internet. O provedor de acesso é livre para estabelecer

o preço de seu serviço prestado e a relação existente entre o provedor de acesso e o usuário é, inequivocamente, relação de consumo, na medida em que está presente a remuneração do provedor/fornecedor, através de um contrato de adesão. Suas atuações são majoritariamente regradas pela ANATEL. Logicamente, sobre esta relação incidirão as normas e princípios os quais preveem os arts. 12 e 20 do Código de Defesa do Consumidor e caso ocorra algum dano pela má-prestação de serviços dos provedores de acesso, estes devem responder objetivamente pelos seus próprios atos, porém devendo-se analisar cada caso. Geralmente, os casos de indenização por sérios problemas de conectividade são impetrados contra os provedores de acesso e não contra os de *backbone*. No tocante à responsabilidade civil, é importante destacar que a jurisprudência tem se posicionado no sentido de não reconhecer o dever de o provedor de acesso reparar os danos causados por atos de terceiros. Contudo, haverá responsabilidade subjetiva, fundamentada no art. 19 do Marco Civil da Internet e no art. 186 do Código Civil, quando os provedores de acesso deixarem de interromper a prestação dos serviços utilizados pelo usuário que pratica atos ilícitos, desde que tenham sido previamente informados e que não restam dúvidas sobre a ilicitude da conduta, especialmente se houver um mandado judicial (SÁVIO, 2013, p. 55). Com dados de 2015 (BOECHAT, 2015), os principais são: Algar Telecom (aproximadamente 444 mil assinantes); Oi (aproximadamente 6,5 milhões de acessos e 25,5% do mercado); Sky (aproximadamente 216 mil acessos); Live TIM (aproximadamente 206,3 mil assinaturas); Vivo (aproximadamente 4 milhões de assinaturas); NET Virtua (maior provedora no Brasil com 32% de todos os assinantes de internet no país); GVT; dentre outras.

O provedor de hospedagem é aquele que oferece serviços de armazenamento de dados em servidores próprios de acesso remoto, possibilitando o acesso de terceiros a esses dados, de acordo com as condições contratualmente estabelecidas. Assim, fornece dois tipos de serviço: o armazenamento de arquivos – dados – em servidor de acesso remoto e o acesso a esses arquivos armazenados. Geralmente todos os tipos de provedores, especialmente os de conteúdo e informação, também são provedores de hospedagem, para que haja a devida dinâmica e guarda de informações e dados pessoais que o próprio MCI e a LGPD demandam que guardem. E para o provedor de hospedagem se incide a mesma teoria de responsabilidade, de só caber indenização se este descumprir decisão judicial, com o seu consumidor-usuário. Temos os exemplos: Google Drive e Dropbox.

Os provedores de conteúdo e os de informação funcionam como intermediários entre o editor de conteúdo de um site e o usuário que acessa as publicações nele veiculadas. Trata-se, pois, da pessoa jurídica ou natural que fornece o material a ser difundido na rede, mediante oferta ao público de produtos ou serviços colocados à disposição do consumidor. Este provedor

é responsável pela criação das informações divulgadas por meio da internet. Importante frisar que o provedor de conteúdo pode ou não ser o próprio provedor de informação, na medida em que seja ou não o autor das informações disponibilizadas (LEONARDI, 2005, p. 283). Sendo importantíssima esta definição no momento da averiguação da responsabilidade civil que incide em cada caso a ser analisado. Se o provedor de conteúdo intervier na comunicação, dando-lhe origem, revisando e editorando previamente ou escolhendo ou modificando o conteúdo ou selecionando o destinatário, responderá objetivamente perante o consumidor-usuário pelos danos a este causado, incidindo o art. 21 do Marco Civil:

Art. 21. O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. (BRASIL, 2014).

Todavia, estes dois tipos de provedores são distintos. O provedor de informação é responsável por toda publicidade e anúncio constante na internet, ele é o autor; o provedor de conteúdo é quem analisa a publicidade e a divulga na rede, quem disponibiliza a informação. Não havendo necessidade de maiores distinções, pois as incidências jurídicas são as mesmas. Como vimos, em relação à responsabilidade civil dos provedores de conteúdo e informação deve-se considerar se o dano é por atos próprios ou por atos de terceiros. Quando o conteúdo for próprio do provedor, incide a responsabilidade objetiva, mediante Código Civil e Código de Defesa do Consumidor, bem como nas legislações específicas às particularidades de cada ato danoso. Caso o ato ilícito seja praticado por terceiro e caso tenha exercido algum tipo de controle editorial prévio, subentende-se responsável de forma concorrente. O provedor de conteúdo exime-se da responsabilidade quando não há controle editorial prévio, sendo responsável somente em casos de omissão, quando não bloqueia o acesso ou deixando de remover o conteúdo ofensivo em razoável e legal prazo, quando comunicado ou conhecido o ato ilícito (SÁVIO, 2013, p. 55). Temos por exemplo: Facebook e YouTube.

O provedor de correio eletrônico já possibilita a troca de mensagens entre os seus usuários, reservando-lhes uma “caixa postal” no servidor para armazenar as mensagens recebidas, cuja recepção será devidamente comunicada ao usuário, além de enviar os e-mails por este originado e permitir seu acesso a estes e-mails (LEONARDI, 2005, p. 287). Quase sempre será objetiva a responsabilidade civil, mediante os arts. 12 e 20 do CDC, quando se trata de ato próprio do provedor. No tocante à responsabilidade por atos de terceiro, a jurisprudência dominante tem entendido que o provedor será solidariamente responsável com o autor do dano,

caso esse pudesse ser evitado, nos casos em que, por exemplo, deixar de informar os perigos decorrentes de uma invasão, por não manter atualizados seus equipamentos e programas de proteção ou por não rastrear o autor do ato lesivo e puni-lo com o fornecedor de serviço, caso seja legítima a punição (SÁVIO, 2013, p. 56). Por exemplo temos: Hotmail e Gmail.

A classificação do provedor de comércio eletrônico não é usual. Geralmente ele está incluso na classificação de conteúdo ou de hospedagem, mas sua crescente regulamentação e importância merece sua separação. Inclui-se aqui os *e-commerces*, os comércios eletrônicos na internet que possuem site para a comercialização de suas próprias mercadorias ou serviços onde ocorre a compra e venda de bens e serviços numa relação direta entre fornecedor e consumidor, e os fornecedores de intermediação, que atuam disponibilizando a plataforma e o sistema de venda desenvolvido para a negociação de produtos e serviços por terceiros (funcionando como *marketplaces*). Além desses dois, podem existir outras formas de comércio eletrônico (como nas plataformas de economia participativa), não se excluindo a possibilidade de haver outras combinações entre os tipos de provedores. A responsabilidade recai sobre ele se o dano for de origem do próprio provedor; caso o dano for de terceiro, segue a regra de que não recairá responsabilidade exceto se não tiver excluído o conteúdo ou indisponibilizado o produto após notificação ou decisão judicial. Todavia, esta categoria abrange uma série de problemas os quais ainda, como naqueles casos em que marketplaces ganham uma porcentagem ou valor por venda. Temos como exemplos de: *e-commerces*, todos sites que disponibilizam seus próprios produtos; e *marketplaces*, OLX, Mercado Livre e o *Marketplace* do Facebook.

Por fim temos os provedores de pesquisa, aqueles cuja atividade é a procura na web por determinada informação requerida pelos usuários, fornecendo os resultados existentes. Se um usuário pretende acessar um site ou informação, mas não conhece seu domínio ou algum site específico para aquele assunto, ele pesquisa, fornecendo palavras, frases ou outros materiais. Assim, sua atividade não cria dados nem é, primariamente, veículo de divulgação de informações de terceiros, mas sim, trata-se de um catálogo dos conteúdos disponibilizados por outros provedores. Esta classificação, assim como dos provedores de pesquisa, também não é comum e sua incidência de responsabilidade civil é a mesma, devendo responsabilizar-se em relação aos danos causados pelos conteúdos resultantes das suas buscas quando tinha o conhecimento do mesmo. Lembrado que não há responsabilização desse provedor e do de correio eletrônico, na hipótese de conteúdo ilícito gerado por terceiros, devido às suas características únicas da atividade e ao sigilo das comunicações, respectivamente, que seriam isentos de responsabilidade ainda que ignorassem a notificação do ofendido, não podendo ignorar, porém, o mandado judicial. Exemplos deles são: Google, Yahoo, Bing e DuckDuckGo.

Assim, a responsabilidade de um provedor de internet variará de acordo com o tipo de serviço prestado (*backbone*, acesso, conteúdo, informação, hospedagem, correio eletrônico, comércio eletrônico e pesquisa), com o evento analisado, com as cláusulas contratuais estabelecidas com o consumidor e com as normas que as tutelam. Lembrando que são raros os casos em que um provedor de serviço será inteiramente de um só tipo.

### **2.3.4 Perecividade das Provas de Cibercriminosos**

*São necessários pouquíssimos segundos para que o cibercriminoso possa apagar todos seus rastros digitais.*

Por causa da virtualidade dos dados na rede, todas informações são inerentemente artificiais e, logo, manipuláveis pelo ser humano. E por causa do altíssimo desconhecimento das massas sobre aspectos técnicos da rede e por conta do abuso sem reprimendas de quem tem estes conhecimentos, cibercriminosos dificilmente são identificados e condenados. Atualmente, a Polícia Federal zela – como deve – da coleta e guarda das provas a fim de evitar alterações e quebra de integridade, para que as provas verificadas continuem o mais próximo possível como foram encontradas. Porém, muitas provas contra cibercriminosos se utilizam de mecanismos de criptografia e que, às vezes, só podem ser averiguadas quando o equipamento está ligado, onde podem sofrer pequenas alterações e, logo, perda de provas cruciais.

No procedimento de perícia de uma arma de fogo, por exemplo, deve ocorrer o disparo com a arma em ambiente de laboratório para analisar a prova do possível crime, ao ser efetuado o disparo da arma ocorre uma alteração de provas. Isso não significa que a prova seja modificada a ponto de tornar-se inadmissível, porém, a mesma precisa ser preparada para a análise. E por que isso não é contestado? Devido ao método utilizado ser cientificamente comprovado e reconhecido. Isso também ocorre, por exemplo, na coleta de digitais que estão presentes em uma cena de crime, onde só é possível a coleta através do uso de instrumentos digitais, os quais são utilizados para perpetuar a prova, sem danificá-la, em que as coletas de evidências de cibercrimes devem ter a devida admissibilidade, comprovação e reconhecimento em tribunais já que se trata de crimes novos a serem investigados (COSTA, 2008, p. 11-12). Devem ser tomadas algumas precauções a chegar-se à cena do cibercrime para garantir a integridade das evidências, tentando não modificar, desligar equipamentos ou obter provas, a menos que os mesmos sejam treinados em forense computacional, pois muitos criminosos

podem deixar cavalos de Tróia e outros mecanismos que programem a destruição das provas do equipamento assim que sejam desligados ou manipulados incorretamente (COSTA, 2008, p. 27).

Esta característica é essencial, por exemplo, na interpretação da desnecessidade de mandados judiciais em alguns casos de cibercrimes, afinal, são necessários pouquíssimos segundos para que o cibercriminoso possa apagar todos seus rastros digitais ou, no mínimo, submetê-los a rigorosos mecanismos de criptografia (ALVES, 2019b).

### 2.3.5 Desconfiança Generalizada

*Não há total confiança na comunicação virtual.*

Lessig (1999, p. 28) chama esse fato de imperfeição. Esta consequência do grande dinamismo e incertezas do meio digital faz com que o comércio eletrônico não se desenvolva ainda mais já que não há total confiança na comunicação virtual. Normalmente, não há desconfiança quando enviam e-mails, acessam sites para a leitura de jornais, de blogs de opinião ou de notícias. Pelo contrário, muitos desconfiam até pouco demais como as “tias(os) do WhatsApp”, termo que designa as pessoas que inadvertidamente consomem e distribuem informações imprecisas e que acreditam em tudo que lê nas redes sociais e apps de mensagens. Essas pessoas são mais susceptíveis a acreditar em mentiras e não conseguem determinar uma afirmação genérica. Decresce um pouco o número de pessoas confortáveis em comprar um livro ou um aparelho eletrônico pela internet. Porém, quase ninguém se arriscaria a adquirir um automóvel ou um imóvel tão somente pela internet justamente porque não nos sentimos seguros o suficiente a respeito da garantia da autoria ou integridade da mensagem ou da declaração de vontade ou até se o documento eletrônico – o contrato – que tenha viabilizado a transação será aceito como meio de prova. Como o limite do valor médio desses produtos tivesse o custo-benefício suficiente para uma atividade criminal. Na realidade, de acordo com a UNCITRAL (da Organização das Nações Unidas - ONU), mensagens pelo meio eletrônico e contratos eletrônicos não têm maior fragilidade do que mensagens e contratos normais, ou seja, eles têm equivalência funcional. Será o julgador quem decidirá a validade e importância das provas e certificados digitais em cada caso. Outro motivo dessa desconfiança é a impossibilidade técnica de saber como seu dado é violado e qual a fonte de um suposto vazamento de certo dado. Vejamos um caso deste exemplo:

EMENTA: APELAÇÃO CÍVEL. AÇÃO DE COBRANÇA. CONTRATO ELETRÔNICO. PRINCÍPIO DA EQUIVALÊNCIA FUNCIONAL. PROVA DA ASSINATURA. ART. 389, II DO CPC. AUSÊNCIA DE DEMONSTRAÇÃO. SENTENÇA MANTIDA. 1. Pelo princípio da equivalência funcional, o registro eletrônico da contratação não lhe compromete a validade nem a eficácia. Contudo, remanescem os cuidados com a inalterabilidade e o registro da declaração de vontade. 2. Nos termos do art. 389, II do CPC, contestada a assinatura do documento, cabe à parte que o produziu provar-lhe a veracidade. (MINAS GERAIS, 2013).

O meio digital pode ser muito volátil e, às vezes, mais suscetível a certos erros que no mundo real-real e em outros casos ele é mais seguro. Suponhamos que em certa loja física, o consumidor quer certo produto de tal cor. Ao pedir verbalmente ao vendedor o produto com estas características, este o entrega já na embalagem e o consumidor não confere. Chegando em casa, depara-se com o erro da cor do produto pelo vendedor. Será mais difícil de comprovar a culpa do vendedor e é obrigação do consumidor verificar tudo isso no momento da compra (quando não se trata de um defeito de desempenho). Já no meio digital, se é selecionada a cor e ela consta no contrato digital ou na nota fiscal, fica muito mais fácil comprovar o erro e culpa do vendedor neste caso. Um desses erros é o equívoco momentâneo do preço em site de comércio eletrônico causado por falha do sistema informático em vista da certa falha de funcionamento dos sistemas de informação, neste caso o consumidor não poderá abusar desse momento pois tratar-se-ia de enriquecimento ilícito já que o princípio da boa-fé objetiva que exige um comportamento leal de ambas partes. Mas caso o preço esteja em um limite aceitável, devido à incomensurável vantagem para o empresário já que a determinação do preço é quase um comando instantâneo, no caso de divergência de preços para o mesmo produto entre os sistemas de informação de preços utilizados pelo estabelecimento, o consumidor pagará o menor dentre eles. É o que comprovam as jurisprudências:

RESPONSABILIDADE CIVIL. RELAÇÃO DE CONSUMO. AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZATÓRIA. COMÉRCIO ELETRÔNICO. ALEGAÇÃO DE VEICULAÇÃO DE PROPAGANDA COM PREÇO PROMOCIONAL NÃO COMPROVADA. ERRO EVIDENTADO PREÇO. PRINCÍPIO DA BOA-FÉ OBJETIVA QUE EXIGE UM COMPORTAMENTO LEAL DE AMBAS AS PARTES CONTRATANTES. CONDENAÇÃO POR LITIGÂNCIA DE MÁ-FÉ QUE SE AFASTA. PROVIMENTO PARCIAL DO RECURSO. (RIO DE JANEIRO (Estado), 2011).

COMINATÓRIA. CONSUMIDOR. COMÉRCIO ELETRÔNICO. AQUISIÇÃO DE COMPUTADOR POR PREÇO PROMOCIONAL. PEDIDO CANCELADO SOB ARGUMENTO DE ERRO MOMENTÂNEO NO SITE. NO CASO EM TELA, A OFERTA NÃO VINCULA O FORNECEDOR, DIANTE DO ERRO SUBSTANCIAL DA PUBLICAÇÃO, PERCEPTÍVEL PELO HOMEM MÉDIO DIANTE DA DESARRAZOABILIDADE DO VALOR OFERTADO. PRINCÍPIOS DA BOA-FÉ E DO EQUILÍBRIO (ART. 4º, III, DO CDC). RECURSO PROVIDO PARA JULGAR IMPROCEDENTE O PEDIDO DO AUTOR. (RIO GRANDE DO SUL, 2009b).

CONSUMIDOR. OFERTA. VINCULAÇÃO. ERRO. PREÇO IRRISÓRIO DE BEM DE CONSUMO. Ar condicionado de 30.000 btus oferecido na rede da internet, no site da loja Submarino.com pelo valor de R\$ 3,00. Aplicável à espécie os princípios da boa-fé, equilíbrio e a vedação ao enriquecimento sem causa, os quais afastam a obrigatoriedade da oferta constante do art. 30 e 35, inciso I, do CDC. RECURSO PROVIDO. (RIO GRANDE DO SUL, 2005).

### 2.3.6 Internacionalização de Condutas

*Usuários podem difamar e discriminar cidadãos de outros países sem sanção legal.*

A última consequência é a internacionalização das condutas, garantida pela “deslocalização” que possibilita o acesso a informações armazenadas em servidores de qualquer local do planeta. Os casos de litígios transnacionais englobando pessoas, físicas e jurídicas, de diferentes países ou de múltiplas jurisdições são bastante frequentes. Neste sentido, houve o emblemático caso Garcia vs. Panasonic, em que o autor ganhou a ação pela aplicação do artigo 12 do CDC, com uma interpretação menos restritiva, conjugado com a teoria do risco e a chamada “teoria da integração” porque “as grandes corporações perderam a marca da nacionalidade para tornarem-se empresas mundiais” e se a globalização beneficiava a Panasonic, deveria, em contrapartida, também beneficiar o consumidor:

DIREITO DO CONSUMIDOR. FILMADORA ADQUIRIDA NO EXTERIOR. DEFEITO DA MERCADORIA. RESPONSABILIDADE DA EMPRESA NACIONAL DA MESMA MARCA (‘PANASONIC’). ECONOMIA GLOBALIZADA. PROPAGANDA. PROTEÇÃO AO CONSUMIDOR. PECULIARIDADES DA ESPÉCIE. SITUAÇÕES A PONDERAR NOS CASOS CONCRETOS. NULIDADE DO ACÓRDÃO ESTADUAL REJEITADA, PORQUE SUFICIENTEMENTE FUNDAMENTADO. RECURSO CONHECIDO E PROVIDO NO MÉRITO, POR MAIORIA. I - Se a economia globalizada não mais tem fronteiras rígidas e estimula e favorece a livre concorrência, imprescindível que as leis de proteção ao consumidor ganhem maior expressão em sua exegese, na busca do equilíbrio que deve reger as relações jurídicas, dimensionando-se, inclusive, o fator risco, inerente à competitividade do comércio e dos negócios mercantis, sobretudo quando em escala internacional, em que presentes empresas poderosas, multinacionais, com filiais em vários países, sem falar nas vendas hoje efetuadas pelo processo tecnológico da informática e no forte mercado consumidor que representa o nosso País. II - O mercado consumidor, não há como negar, vê-se hoje ‘bombardeado’ diuturnamente por intensa e hábil propaganda, a induzir a aquisição de produtos, notadamente os sofisticados de procedência estrangeira, levando em linha de conta diversos fatores, dentre os quais, e com relevo, a respeitabilidade da marca. III - Se empresas nacionais se beneficiam de marcas mundialmente conhecidas, incumbe-lhes responder também pelas deficiências dos produtos que anunciam e comercializam, não sendo razoável destinar-se ao consumidor as consequências negativas dos negócios envolvendo objetos defeituosos. IV - Impõe-se, no entanto, nos casos concretos, ponderar as situações existentes. V - Rejeita-se a nulidade arguida quando sem lastro na lei ou nos autos. (BRASIL, 2000).

Em suma, era uma empresa grande contendo a venda e propaganda do mesmo produto em ambos países com sedes em ambos países, um caso bastante específico. Inobstante, a maioria dos casos permanece sem uma solução legislativa eficaz: empresas com sede em um só país, comercialização por exportação/importação, compra e venda de produtos em outros países, disponibilização do produto num só país estrangeiro etc. Mas quando estes casos chegam nas cortes brasileiras, cada jurisdição tenta uma solução diferente. Por exemplo, embora o princípio da territorialidade seja base do sistema de direitos autorais na Internet, sua aplicação ainda não é clara pela descentralização da atuação das plataformas.

Luiz Alberto Albertin (2004, p. 47) categoriza as formas de relação jurídico no âmbito contratual no meio digital em: B2B (*business to business*), em que os usuários são compradores e também empresários em uma relação de contrato de consumo entre duas empresas (como a disponibilização de produtos de outras empresas no site de outras como no da Magazine Luiza); B2C (*business to consumer*), em que os internautas são consumidores que adquirem os produtos das empresas através de websites (o mais comum); C2C (*consumer to consumer*), negócios feitos entre os próprios indivíduos-consumidores que ofertam algum produto ou serviço através de uma plataforma intermediária (como na OLX); G2C (*government to citizen*), o governo fornece produtos e serviços ao cidadão (como certidões digitais ou processo eletrônico); G2B (*government to business*), o governo contrata fornecedores de produtos ou serviços através das licitações (como no pregão virtual); e G2G (*government to government*), com as relações entre agências governamentais.

Além dessas relações contratuais e consumeristas, há a interação entre pessoas físicas de países distintos com litigâncias penais ou cíveis. Observemos a gravidade deste problema: usuários podem difamar e discriminar cidadãos de outros países sem sanção legal, tampouco incidindo responsabilidades trabalhistas, ambientais ou tributárias. Tal peculiaridade esclarece até mesmo a atual crise do conceito de cidadania e o fim do Estado-Nação. Como solução utópica, Marcelo Neves (2009, p. 111) leciona sobre as “aldeias jurídicas globais”, uma *lex digitalis*, englobadas estruturalmente com sistemas mundiais através de Constituições civis (TEUBNER, 2003).

## 2.4 DIREITO DIGITAL COMO DIREITO REGULATÓRIO

*Talvez a lógica de mercado seja perfeita, mas seus atores não são.*

Vimos o grande paradigma que enfrenta o Estado nos tempos atuais. Como pode ser o Estado uma força restritiva que garante a liberdade? Questiona-se se é possível produzir justiça a partir de critérios técnicos e contingentes, baseados só em resultados. E destes resultados, se deduzir quais são os modelos regulatórios mais benéficos ao povo. Niklas Luhmann (1979, p. 64) sustenta que a produção da legitimação do sistema jurídico surge a partir da justiça que só poderá ser produzida – se fazer visível – a partir dos seus resultados. Trata-se de uma visão de justiça que depende de sua eficácia.

Para Hobbes, regras devem ser eficazes, justas e necessárias. Encontrando-se aí o primeiro problema geral do embate entre Intervencionismo e Liberalismo, o véu humano – de experiências e pontos de vista sobre os mesmos eventos – por trás de cada visão sobre algum aspecto pelo qual o Estado deve ou não intervir, tutelar ou regulamentar. Vejamos que, para ele:

A lei não foi trazida ao mundo para nada mais senão para limitar a liberdade natural dos indivíduos, de maneira tal que eles sejam impedidos de causar dano uns aos outros, e em vez disso se ajudem e unam contra o inimigo comum. [...] uma boa lei é aquela que é necessária para o bem do povo e além disso evidente. Pois o objetivo das leis (que são apenas regras autorizadas) não é coibir o povo de todas as ações voluntárias, mas sim dirigi-lo e mantê-lo num movimento tal que não se fira com seus próprios desejos impetuosos, com sua precipitação, ou indiscrição, do mesmo modo que as sebes não são colocadas para deter os viajantes, mas sim para conservá-los no caminho. (HOBBS, 2003, p. 116).

Para o presente autor, a princípio, o Estado deve intervir o menos possível no mercado, atuando somente quando necessário. Como escreve Offe (1984), quanto mais a política se fizer concreta, tanto mais se multiplicarão os conflitos e se acentuarão os efeitos da polarização. Estará, assim, aberto o caminho à crise política, devido à incapacidade de coordenar satisfatoriamente todos os interesses do complexo social ao mesmo tempo. Além disso, surgirá para o Estado o problema da legitimação, ou seja, do consenso acerca dos critérios qualitativos que orientam suas intervenções, já que o Estado tem que enfrentar a perda de controle social, que se manifesta essencialmente como crise de motivação em relação aos valores tradicionais do individualismo e do profissionalismo, pondo em ação uma ampla rede de vigilância e controle pela ampliação do aparelho policial e pelo incremento de vastos setores do chamado trabalho social (HABERMAS, 1975).

O Direito Digital a ser construído pelo Estado deve: promover a racionalização e a interoperabilidade tecnológica dos serviços de governo eletrônico, permitindo o intercâmbio de informações e a agilização de procedimentos; incentivar a adoção de padrões de formatos abertos, com a disseminação de informações públicas de forma aberta e estruturada; otimizar a

infraestrutura das redes; promover a qualidade técnica da inovação dos serviços de internet, sem prejuízo à abertura e neutralidade; apresentar diretrizes para o ambiente cibernético; propiciar a livre concorrência e a iniciativa privada; otimizar a infraestrutura das redes, favorecendo a qualidade técnica e inovação de serviços; disciplinar o conhecimento para o uso da internet como ferramenta de exercício de cidadania, promoção de cultura e desenvolvimento tecnológico; simplificar os serviços eletrônicos e não apenas exigir novas obrigações fiscais. Uma rigidez jurídica limitaria as liberdades individuais dos cidadãos com base em valores axiológicos de coibição de autonomia e garantias fundamentais (FONSECA, 2011).

É evidente que cada governo deve ter uma estratégia de segurança cibernética, com tutelas jurídicas para a proteção do usuário e separação das normas de intervenção econômica-estatal. Por exemplo, podem haver restrições à compra de software e a outros produtos de TI de fornecedores estrangeiros ou a imposição de requisitos de testes desnecessários os quais criariam barreiras à venda de produtos de TI estrangeiros. Estas restrições dificultam a permeação de produtos que podem oferecer melhores soluções do que àquelas que empresas brasileiras possuem.

Em economia, o intervencionismo se caracteriza pelas ações do Estado que condicionam a atividade econômica do país mediante a regulação do mercado, com a fixação de preços e salários, controle do mercado de câmbio ou estatização de setores, possibilitando ao Estado ser produtor de bens e serviços. A avaliação do intervencionismo econômico varia de acordo com diversas correntes. Em geral, o intervencionismo é caracterizado quando as tendências do mercado são negativas, devendo as mesmas serem mitigadas ou controladas pelo Estado. A defesa de medidas intervencionistas ou de controle de mercado – exceto o caso de considerarem o Direito em si uma forma de intervenção – não é a proposta de análise do presente trabalho porque não há uma tendência de mercado negativa economicamente a ser solucionada aqui. Na verdade, o objetivo é encontrar soluções, não de problemas econômicos de mercado, mas dos problemas práticos encontrados pelos usuários na internet.

O termo liberal se revela ambíguo e banalizado, pois o termo é usado em contextos disciplinares bastante diversos entre si. Em suma, a decisão acerca da nocividade, ou não, desta ou daquela liberdade natural, bem como o consequente controle social levado a efeito pelo direito, deve ser uma resposta à opinião pública e às formas institucionais. De acordo com Keynes, os sistemas políticos democrático-liberais demonstrariam na prática sua superioridade assegurando, ao mesmo tempo, um máximo de eficiência econômica, justiça social e liberdade individual. A tendência do Liberalismo contemporâneo é evidenciar a incapacidade dos Estados-burocráticos para resolver questões sociais pelo fatal desvio das funções prefixadas,

com a formação de uma nova classe corrupta agindo em função de seu próprio interesse, e por haver uma contradição intrínseca entre a lógica das máquinas burocráticas e a lógica da participação (mercantil). Ou seja, este liberalismo anti-utilitarista acredita que a resposta aos problemas da justiça e da segurança social seja dada ao nível da sociedade civil e não ao nível institucional-estatal, mediante subsistemas autônomos do sistema político e iniciativas independentes e convergentes, realizadas por forças sociais espontâneas, e não mediante ações administrativas. Em outras palavras, o problema histórico, que atualmente agita o pensamento liberal, é a adaptação a novos contextos da função anteriormente desenvolvida pelas autonomias locais contra o Estado burocrático-centralizador. E mesmo no pensamento mais liberal, exceto no ilusório anarcocapitalismo, o Estado ficaria apenas com a tarefa de garantir para todos a lei comum, bem como a função de órgão equilibrador e incentivador de iniciativas autônomas da sociedade civil. Esta é a lógica pela qual o Liberalismo, em geral, é regido e doutrinado (MATTEUCCI, 1998, p. 703-705).

Porém cada caso deve ser particularmente analisado, verificando-se cada aspecto econômico para se saber se Estado deve ou não intervir, observando as variáveis e outros contextos internacionais históricos. Na análise geral, o presente autor tem a percepção de que inúmeros contextos econômicos podem ser facilmente autorregulados pelo mercado sem a necessidade de intervenção estatal, muitas dessas lógicas de mercado são notadas na prática. E com certeza, no Brasil, existem burocracias intervencionistas demasiadas para o tamanho benefício que pregam. Mas no contexto do ciberespaço são notórios os atos ilícitos praticados a serem regulamentados e solucionados. Não (exclusivamente) econômicos, mas sim jurídicos. Não obstante, os problemas jurídicos, como normas que somente tutelam atos ilícitos, influenciam sim logísticas de mercado, mesmo que de forma mínima e indireta, porém a manutenção dos direitos fundamentais e humanos do cidadão deve ser a prioridade. Há muitos que, no pensamento liberal, não veem a necessidade de diversos ordenamentos jurídicos, demasiadas normas e controles, como por exemplo o Direito Trabalhista. A maioria dos argumentos são fundados não na concepção de que todo direito é um intervencionismo ruim em si – apesar de muitos assim pensarem –, mas sim de que na prática, por exemplo no caso do Direito Trabalhista, o mínimo que a mesma tutela e impõe o qual o trabalhador deve obter, pode ser obtido de forma natural caso não houvesse tamanhos intervencionismos. Porém, alguns vícios da generalização destas análises não de ser citados.

Em um mercado de trabalho genuinamente livre, na concepção liberal, o Estado deveria ser neutro às relações trabalhistas, exceto por adjudicar disputas, exigir cumprimento de obrigações contratuais e punir fraudes e violência contra pessoas ou propriedades.

Trabalhadores individuais estariam livres para negociar diretamente com seus empregadores ou poderiam se juntar para oferecer seus serviços como um grupo. A descrença nos direitos trabalhistas normalmente se justifica porque os liberais não costumam enxergá-los como um benefício real aos trabalhadores. Usando até da comparação de países com maior índice de liberalismo trabalhista tendo melhores resultados econômicos. Porém, esta análise econômica do Direito Trabalhista merece uma série de cuidados. Por exemplo, a crítica que se faz a esta mesma lógica no Direito Digital, que a oferta sempre oferece eventualmente o que a demanda precisa, nem sempre acontece, por insuficiência de empresas no combate dos principais crimes cibernéticos os quais atingem os usuários.

Enfim, quando criticados seus contextos idealizados imperfeitos, liberais culpam tão somente o contexto da presença estatal, como a presença do imposto por exemplo já que o mesmo diminuiria a geração de empregos devido aos seus custos, o que sufocam a livre concorrência, diminuindo clientela e seus lucros, fazendo com que, assim, hajam mazelas trabalhistas. Mas a lógica de que a falta de dinheiro por conta de deveres estatais é a culpada do maltrato de empresas não ocorre na prática. Ao contrário, problemas trabalhistas ultrapassam problemas estatais, porque o empregador-empresário, mesmo nas melhores das intenções, acaba por muitas vezes cometer atos ilícitos a serem retratados. Deve-se notar que há problemas de mercado independentes da presença do Estado. Talvez a lógica de mercado seja perfeita, de que ele supre todos problemas pela dualidade da oferta-demanda, mas seus atores em meio às suas interações não o são.

Quando economistas tratam a Economia como uma ciência exata e, buscando adaptar suas abstrações à própria realidade, uma teoria não prevê corretamente a realidade, a culpa é atribuída a algum aspecto negativo da sociedade e não à teoria. Até porque isto indicaria que eles não detêm toda racionalidade que proclamam dominar. Em resumo, economistas, intervencionistas ou liberais, erram logicamente ao generalizarem a partir de casos específicos, ao induzirem inconsequentemente – para liberais, como se tudo que o Estado fizesse fosse ruim, e para intervencionistas, como se toda abstenção estatal levasse à desigualdade – e ainda abusam de discursos de autoridade, como se fossem profetas dos problemas socioeconômicos. Explica-se aqui os atuais extremismos políticos presentes no debate sobre qual o melhor modelo regulatório. Em todo o mundo, cada bloco – intervencionista ou liberal, geralmente no escopo político direita-esquerda – enxerga o outro como um intérprete simplista, incoerente e ignorante da realidade cujo causa-efeito só eles veem, com tamanha providência intelectual. Estes jamais considerariam a possibilidade de que algumas de suas interpretações estejam enganadas. É visível nos debates em que economistas de certas bandeiras orgulham-se dos dados positivos

de seu país por certa política de intervenção ou não, sempre se despreocupando com a realidade da população. A alienação é tamanha que, caso indagados, não apresentam novos fatos, mas sim categorizam o adversário como ignorantes e pessimistas, enfim, tudo aquilo que os adoradores do *status quo* mais gostam: aplicam sentimento de culpa nos não-contribuintes, adoram a aparência – e o menos possível a realidade – e justificam que seus meios valerão a pena para utópicos fins.

Para Ellul (1990), escolher um sistema preferido é escolher um álibi que permite ao indivíduo recusar a tomada de uma decisão individual transformadora. Defensores de qualquer sistema desconhecem todas especificidades da Economia ou do Estado. Por isso, ao clamarem saber qual o melhor sistema, livram suas consciências de suas responsabilidades perante esta complexidade. Afinal, predomina-se a ideia de que a autorreflexão e a ação individual em nada resultam, sustentando-se na aparência de que só há a escolha entre o capitalismo e o comunismo ou entre o intervencionismo por políticas públicas e o liberalismo de mercado.

Na vida privada, a esperança da maioria inserida no meio digital é a de que seja ele(a) um sortudo ou um trabalhador que – por algum poder, conhecimento, “viralização” ou dinheiro – se desvencilhe dos males naturais da Economia, através de seus milhares ou milhões de “seguidores”. Nos é pregado que todos somos potenciais empresários, lutadores pela carreira ou funcionários com potencial, todos creem ter potencial para ser especial e diferente. E aqueles que não se destacam na Economia digital são fracassos do *copywriting*. Este ideal liberal pregado na internet não parece saudável para o indivíduo.

São complicadas as soluções de todos problemas da técnica na Economia. O sistema econômico de hoje é muito diferente do que existia a 30 anos atrás e é impossível prevê-la daqui 30 anos. Muda-se até o dinheiro, como as criptomoedas, que não serão a última mudança na sistematização computacional da troca. Se resta impossível prever – para controlar – o futuro, quem dirá o futuro da internet. Podemos apenas mudar as configurações das empresas provedoras de hoje, como no uso consciente dos dados pessoais em que a dificuldade é a falta de limitação de sua coleta pelas empresas quando não há fiscalização efetiva. É difícil nos livrarmos da tendência puramente lucrativa em prol de uma ética intangível.

Um dos principais problemas destas críticas é a pergunta: por que as leis trabalhistas, que somente exigem condições mínimas ao trabalhador, são impeditivas para que empresários ofereçam mais que o mínimo? Não há lógica neste raciocínio. Lembrando que o presente autor somente defende intervencionismos econômicos quando necessário, contextos raríssimos. Já tratando do Direito como forma de intervencionismo social, há de se fazer melhores análises já que, para concluir que afastar a asseguuração de direitos por lei é algo positivo e que uma simples

lógica de mercado consegue supri-lo, são necessários vários estudos para se retirar a tutela estatal de um ator tão insuficiente no mercado, o trabalhador. A exigência de um tratamento mínimo pela lei não deve ser impeditiva de melhores tratamentos de empresas. Nunca foi e nunca será.

E por que esta preocupação em exhibir a importância do Direito Trabalhista na tutela e segurança do trabalhador? Porque muitos destes raciocínios podem ser utilizados na crítica ao nascimento do Direito Digital. Afinal, são demasiadas as críticas sobre a tutela do objeto principal do Direito Digital, a internet, e muitas delas procedem. A intervenção na internet tem seus riscos assim como a intervenção estatal no mercado. Há normas que tratam da neutralidade da rede no MCI, as quais podem funcionar como uma intervenção econômica e que podem colocar em risco, observando caso a caso, a integridade e até mesmo a dinâmica do mercado digital. Já outras normas somente funcionam para tutelar os atos jurídicos perfeitos e outras para prevenir ciberataques. E como já explicado na comparação com o Direito Trabalhista, na legitimidade do Direito e na imprescindibilidade estatal, a tutela de atos ilícitos – mesmo que influenciem indiretamente no mercado – devem prevalecer pois os direitos fundamentais são prioridades sobre o aspecto econômico. O Direito Digital não deve ter cunho diretamente intervencionista na economia, mas deve atender à necessidade de novas normas e políticas públicas.

Como vimos, a oferta e demanda, no mercado capitalista, tem sim sua lógica e dinâmica, mas não é e nunca será absoluta e mediante falhas humanas, como é de se esperar, encontram-se diversos problemas a serem tutelados. Por exemplo, culpa-se o Estado pelo maltrato aos trabalhadores pelas empresas, como se sem a tutela para exigir um mínimo tratamento dos mesmo e cumprimento contratual devido, os empresários tratariam melhor seus empregados e haveriam menos abusos. Uma lógica deturpada para se acreditar e mudar todo um sistema de mercado apostando na boa-fé de poucos empresários. Como pode a exigência do mínimo – tratamento decentemente legal ao trabalhador – ser o maior culpado do não alcance das empresas de oferecer este mínimo? A exigência de um tratamento mínimo ao ciberusuário também não deverá ser um impeditivo da realização deste pelas empresas.

Outro exemplo clássico é o do nosso exímio Direito do Consumidor. Mediante a insatisfação com empresas em geral, por exemplo de antivírus ou de redes sociais, a falha e liberal lógica de mercado supracitada demonstra que o simples deslocamento para outro antivírus ou rede social diminuiria a possibilidade a ciberataques ou melhoraria os serviços de redes sociais. É uma lógica de mercado obscura, em que o ciberusuário só sai perdendo. A oferta não atende na maioria das vezes a pré-requisitos de segurança que nem chegam perto dos que o Estado

pode auxiliá-la a oferecer. Frisando novamente, como pode a exigência do mínimo ao consumidor (como as normas do CDC) ser o maior culpado do não alcance das empresas de oferecer este mesmo mínimo? Na prática, não faz sentido.

Assim, podemos enxergar, até com comparações ao Direito Trabalhista e Consumidor, algumas das divergências que o Direito Digital pode ter nos seus mais ínfimos fundamentos. Quanto ao Direito Regulatório, seu objeto de estudo é a regulação em si mesma. É, portanto, relevante, para o entendimento do objeto do direito regulatório, o estudo das espécies de regulação (ARANHA, 2014, p. 69). Sendo uma delas a regulação da internet. O mercado deve ser protegido, respeitando o direito à igualdade de condições concorrenciais. A regulação é uma necessidade da constatação de que o próprio Direito e a sociedade criaram entes que desequilibram as relações humanas de acumulação de capital, técnicas e vantagens competitivas, exigindo, portanto, a regulação. E não, como muitos pensam, por consequência de deficiência do meio privado e concorrencial já que é insuficiente por sua natureza:

O pressuposto do Estado Regulador é a intervenção estatal como garantia de preservação das prestações materiais essenciais à fruição dos direitos fundamentais, sejam elas prestações de serviços públicos ou privados, sobre as quais se aplica a insígnia da regulação, ou sejam elas outros tipos de atividades, tais como o exercício do poder de polícia, atividades de fomento e prestações positivas tradicionais de índole concreta e normativa. (ARANHA, 2014, p. 21-22).

A chamada desregulação, eventualmente proposta em um determinado setor, não significa a extinção da regulação, mas tão somente a subtração de uma dimensão da regulação estatal. Assim, o argumento da desregulação nunca poderá ser o de que o setor funcionaria melhor sem intervenção estatal (ARANHA, 2014, p. 88). Razão demasiadamente presente em discursos políticos e econômicos nesta espécie de discussão teórica. O fundamento para uma desregulação resulta de uma ponderação sobre os ganhos sociais oriundos da diminuição da regulação estatal voltada à compensação social, resultando “em maior eficácia dos direitos fundamentais envolvidos” (ARANHA, 2014, p. 88). O exemplo da internet é marcante para evidenciar a insuficiência do mercado como um ente vivo inteligente e eficiente, em vez de entendê-lo como um produto da atuação regulatória capaz de formatá-lo em benefício geral de todos direitos fundamentais. Assim, a regulação é a reconfiguração conjuntural do ambiente socioeconômico voltada à construção do funcionamento do sistema de mercado espelhado nos direitos fundamentais. Podendo aplicar, neste sentido, a conceitualização da regulação e as diretrizes do Direito Regulatório à justificação e perpetuação do Direito Digital, promovendo por meio deste novo Direito regulamentações necessárias à manutenção do bem-estar social na internet.

## **CAPÍTULO 3 ANÁLISE DOS PRINCIPAIS DILEMAS PRÁTICOS E TÉCNICOS NA REDE**

### **3.1 COLISÃO DE DIREITOS E PRINCÍPIOS: PRIVACIDADE, LIBERDADE DE EXPRESSÃO, LIBERDADE DE IMPRENSA, TUTELA DA AVERIGUAÇÃO DE INFORMAÇÕES E SEGURANÇA JURÍDICA**

*Não há bens jurídicos que contenham conteúdo de direito absoluto.*

A presente parte do capítulo três abordará os conflitos de direitos fundamentais e de princípios na era digital. A globalização da internet traz uma liberdade que, muitas vezes sem regulamentação, facilita o conflito de direitos fundamentais. Identificaremos as formas desses conflitos e buscar técnicas que nos orientarão na resolução deste problema de Direito Digital, traçando critérios específicos para tais conflitos. O primeiro direito é a liberdade de expressão, que se funda no princípio da dignidade da pessoa humana como fator limitante desse direito. Diante de sua amplitude, atua como requisito necessário à concretização e aperfeiçoamento do regime democrático e dos demais direitos fundamentais. É por meio da liberdade de expressão que emergem o pluralismo de ideias, a oposição ao governo, a liberdade de imprensa, o direito de educar e de ser educado, a crítica, a opinião e a denúncia. A liberdade de expressão é, portanto, parte vital da democracia. Afinal, sem liberdade de expressão não há democracia e sem democracia não há liberdade de expressão, já que o desenvolvimento do ser humano depende da boa comunicação com os outros para a formação e definição de sua personalidade, respeitando sempre os direitos alheios. E a riqueza do dilema deste subcapítulo é justamente obter um controle das invasões de privacidade sem a supressão do direito à informação e ofendendo o mínimo possível a liberdade de expressão.

Ninguém é capaz de defender uma ideia ou propagar uma informação ou dado sem se desvencilhar de suas ideologias ou valores culturais e políticos e é impossível agradar a todos públicos, de tal maneira que uma ideia ou informação sempre atingirá e alcançará pessoas as quais tais dados não lhes agradarão. Em termos práticos, a assertiva democrática já mencionada, que “cada indivíduo possui direito igual à mais ampla liberdade possível, compatível com a igual liberdade dos outros”, deve ser interpretada de forma específica.

Já o direito à privacidade configura, além de um direito fundamental, um direito da personalidade, essenciais e inerentes à pessoa. Assim, o direito à privacidade visa proteger não somente um indivíduo específico, mas toda uma sociedade por meio de delimitações de onde

começa e onde termina o direito de cada indivíduo. A falta de regulamentação e a ausência de tecnologia adequada para combater os casos de violação da privacidade na internet dificultam a prevenção e repressão a estes atos ofensivos:

Esse quadro é particularmente preocupante em relação a privacidade, cuja violação é exponencialmente facilitada pelas mesmas características e peculiaridades que tornam a Internet tão atraente, a tremenda facilidade de disseminação, de busca e de reprodução de informações em tempo real, sem limitações geográficas aparente. (LEONARDI, 2005, p. 42).

Já sobre o direito à intimidade, lembremos da lição de Robert Alexy (2009) ao mencionar, na obra *Teoria dos Direitos Fundamentais*, a Teoria das Esferas que segrega três esferas com decrescente potencial de proteção: a mais íntima, intangível, reservada e protegida da organização da vida privada; a privada, ampla, que abarca intermediariamente o âmbito privado caso não pertença ao mais interno, de conhecimento somente de outras pessoas de confiança; e a social, que engloba tudo o que não pertença às esferas mais privadas ou que não seja de interesse da pessoa excluir do alcance de terceiros, já que uma informação pode estar no meio social sem sua anuência.

A título de exemplo, para observarmos como se derem estes conflitos no começo da Internet no Brasil, a Justiça do Rio de Janeiro mandou, em decisão liminar de uma Ação de Exibição de Documentos, a *Yahoo* e a *Microsoft* revelarem o autor de e-mails ofensivos de 2005 com mensagens difamatórias a um casal e que também enviou ofensas pelo Windows Messenger. Ao conceder a liminar, o juiz afirmou que houve desrespeito ao artigo 5º, inciso IV, da Constituição Federal, que afirmar ser livre a manifestação do pensar, sendo vedado o anonimato:

APELAÇÃO. AÇÃO CAUTELAR DE EXIBIÇÃO DE DOCUMENTOS. RELATÓRIO DE 'LOGS DE IP' DOS ACESSOS EFETUADOS À CONTA DE CORREIO ELETRÔNICO. LEGITIMIDADE PASSIVA. Embora a apelante-ré, Microsoft Informática Ltda., seja pessoa jurídica distinta da sociedade empresária Microsoft Corporation, mantenedora do serviço de correio eletrônico Hotmail, vê-se do contrato social que aquela é por esta controlada, devendo então ser rejeitada a tese de ilegitimidade passiva ad causam, não só porque ambas integram o mesmo conglomerado econômico, mas sobretudo em razão da aplicação da teoria da aparência, à luz do princípio da facilitação da defesa do consumidor, porquanto a diferenciação das pessoas jurídicas que compõem a holding Microsoft não é de fácil percepção à parte vulnerável da referida relação. Ocorre que o art. 1.194 do CC/02, aplicável por analogia ao caso, dispõe que 'o empresário e a sociedade empresária são obrigados a conservar em boa guarda toda a escrituração, correspondência e mais papéis concernentes à sua atividade, enquanto não ocorrer prescrição ou decadência no tocante aos atos neles consignados'. Demais disso, em havendo relação de consumo, o art. 6º, III, do CDC consagra o princípio da transparência e estabelece o dever de informação clara e adequada ao consumidor em todas as fases contratuais, razão pela qual deve o servidor/provedor de correio eletrônico ter o cuidado de propiciar meios de identificar todos os acessos feitos à conta de e-mail do próprio consumidor, haja vista o dever de segurança que o sigilo das comunicações impõe. Parcial provimento do recurso. (RIO DE JANEIRO (Estado), 2016).

O próprio artigo 2º do Marco Civil define que o uso da internet no Brasil tem como princípio básico o respeito à liberdade de expressão, todavia isso não significa que uma lei infraconstitucional modificou o equilíbrio dado pela Constituição visto que nenhum direito é absoluto e nem está acima de outro. Então, quando há uma colisão de dois direitos com a mesma importância, dependendo do caso concreto, um pode se curvar ao outro.

Atingir a internet somente por conta das mazelas sociais pode acabar com a rede livre, sendo necessária a ponderação da necessidade com o impacto. Porém, de nada vale reclamar sobre possíveis limitações na internet sem oferecer melhores soluções. Para o Direito, seria ideal solucionar tais problemas sem atingir a liberdade e privacidade individual. Enquanto uns se ocupam de alertar genericamente para pequenas restrições de liberdade, o Estado deve atingi-la a fim de resolver, de alguma forma, os diversos problemas dos usuários brasileiros. O mundo real-virtual não pode permitir que ocorram violações incessantes aos direitos fundamentais dos indivíduos e o Direito não pode abandonar tais conflitos, sendo que há um anseio social para a criação de regras regulamentadoras da internet.

Devemos levar em conta, assim como em todo o trabalho, as características jurídicas da internet e do meio digital. Assim, diante de todos esses problemas apresentados, deve haver uma releitura do ordenamento jurídico criando-se critérios e regras específicas para disciplinar o tema e deve o intérprete/julgador utilizar os princípios e técnicas que regem tais conflitos no mundo real promovendo uma adaptação para atender às peculiaridades do mundo real-virtual. A internet trouxe uma nova dimensão a este conflito de direitos fundamentais, pois a facilidade de manifestação, a ampla divulgação e acesso e o caráter permanente das informações inseridas na rede permitem um conflito singular difícil resolução.

A primeira relevante propositura de um método de verificação foi uma decisão prolatada pelo STJ, em sede do Recurso Ordinário em Mandado de Segurança (RMS), interposto para contestar acórdão que denegou a ordem impetrada contra decisão do juízo federal, o qual autorizou a quebra de sigilo bancário requerida pelo Ministério Público (MP). Na época, tal decisão teve uma grande conturbação. O relator do acórdão, do então ministro Luiz Fux, entendeu que a quebra para fins de investigação de suspeita de crime financeiro não viola a privacidade do impetrante porque o sigilo bancário não é um direito absoluto. Noutras palavras, diante das circunstâncias, o colegiado do STJ sobrepôs o direito à informação ao direito à privacidade, quebrando o sigilo bancário do autor do mandato. Para os ministros, nesse caso específico, o peso desse primeiro foi maior que o segundo:

EMENTA. RECURSO ORDINÁRIO. MINISTÉRIO PÚBLICO. SIGILO BANCÁRIO. DIREITO RELATIVO. SUSPEITA DE CRIME FINANCEIRO. 1. **A suspeita de crime financeiro, calcado em prova de lesividade manifesta, autoriza a obtenção de informações preliminares acerca de movimentação bancária de pessoa física ou jurídica determinada por autoridade judicial com o escopo de instruir inquérito instaurado por órgão competente.** 2. A quebra de sigilo bancário encerra um procedimento administrativo investigatório de natureza inquisitiva, diverso da natureza do Processo, o que afasta a alegação de violação dos Princípios do Devido Processo Legal, do Contraditório, e da Ampla Defesa. 3. O sigilo bancário não é um direito absoluto, deparando-se ele com uma série de exceções previstas em lei ou impostas pela necessidade de defesa ou salvaguarda de interesses sociais mais relevantes (Vide §§ 3º e 4º do art. 1º e art. 7º da Lei Complementar 105/2001) 4. Recurso ordinário improvido. (BRASIL, 2003, grifo nosso).

Não restando porque falar sobre a veracidade da informação em questão nem o status do autor da ação, vez que são implícitos em casos de quebra de sigilo bancário. São relevantes neste caso o interesse público envolvido na questão e a licitude dos meios de obtenção da informação. No interesse público, a própria ementa supracitada mostra a importância da fiscalização de suspeita de crime financeiro, sendo valor determinante na quebra do sigilo bancário. Já em relação a licitude dos meios de obtenção desta informação, foi válido o requerimento de quebra do sigilo feito pelo MP e autorizado judicialmente.

Assim, nota-se uma propensão lógica à consideração do princípio da liberdade de informação em preferência ao direito à privacidade do indivíduo suspeito de fraude. Essa propensão ocorre porque as vantagens obtidas da supressão do direito à privacidade são maiores do que se o contrário acontecesse, como prega o princípio da ponderação de Alexy (2009). A aplicabilidade ao caso concreto de choque entre o direito à liberdade de informação, privacidade e liberdade de expressão serve apenas como ratificadora de sua imprescindibilidade. Dependerá de cada caso a averiguação de necessidade pública estatal no uso do direito de verificação da informação em detrimento da privacidade de alguns de seus cidadãos. Para isto, deve-se levar em conta a conformidade, a idoneidade, a necessidade, a exigibilidade e a proporcionalidade em sentido estrito. A liberdade de expressão não autoriza que o emissor, seja ele quem for, possa tudo. Não se justifica que alguém ofenda, gratuita e aleatoriamente, a honra de um desafeto por motivos de foro íntimo, sob o efeito protetor da liberdade de expressão. O fim de expressar-se, interagir em sociedade, não pode legitimar excessos desproporcionais e abusivos em sua veiculação (meio). O fim não pode servir como pretexto para ofensas aleatórias, exacerbadas, descontextualizadas que venham a ferir a honra de outrem. Por exemplo, um jornalista não pode, ao divulgar notícia de suposto erro médico, argumentar contra o profissional e adjetivá-lo de imbecil ou monstro. Note-se que esses adjetivos (meios) são

desnecessários à informação (fim), excedendo aos limites da notícia, convertendo-se em ataque pessoal à honra de uma pessoa.

Antes de se implementar qualquer maior relevância a um bem jurídico sobre outro, se deve buscar à exaustão a compatibilização de ambos bens jurídicos. Para este exame deverá o operador do direito, antes de qualquer medida, tentar realizar um diagnóstico dos possíveis efeitos adversos que a medida restritiva-limitativa poderá gerar e avaliar sua necessidade para a solução da matéria. É neste contexto que Robert Alexy (2009, p. 91) adverte que “quanto mais grave é a intervenção em um direito fundamental, tanto mais graves devem ser as razões que o justifiquem”. Assim, a tutela da averiguação de informações e até a restrição de conteúdo, no meio digital, devem ser feitas com a maior cautela possível e só quando necessário. Lembrando que para o combate de ciberterrorista, na prática, quase sempre será preciso invadir minimamente sua privacidade para averiguar provas para verificar a licitude ou não de seus atos e impedi-lo de apagar evidências. Não deve haver outra opção exceto a restrição para evitar um mal maior: a lesão dos Direitos Fundamentais das diárias vítimas dos ciberataques, mediante até o art. 20 do Código Civil (CC).

Em síntese, deve o operador e o juiz do Direito buscar a solução menos excessiva ou drástica e que melhor represente a normatividade. Em todas as três supracitadas dimensões – adequação, necessidade e ponderação em sentido estrito –, deve-se analisar completamente os fatos e contextualizar a via pela qual se exercer a liberdade de expressão e se esta posição pode afrontar outros princípios constitucionais. A Constituição assegura o direito à imagem, à intimidade e à privacidade das pessoas de maneira que a liberdade de expressão em caso de excessos deve ceder de modo a possibilitar o equilíbrio necessário para não violar outros bens jurídicos, igualmente reconhecidos pela Constituição. Nesta perspectiva, poder-se-ia supor que o direito à imagem, à intimidade e à privacidade se sobrepõem à liberdade de expressão. Mas não é necessariamente sempre assim. Em verdade, não há bens jurídicos que contenham conteúdo de direito absoluto. Porém, consoante a máxima democrática de que “cada indivíduo possui direito igual a mais ampla liberdade possível, compatível com a igual liberdade dos outros”, podemos considerar que sempre há a possibilidade de que a segurança e o interesse público, no caso em que são imperiosos através de sua tutela de averiguação de informações, possam ultrapassar a privacidade do indivíduo para a devida consolidação e segurança jurídica, bem como é possível restringir certas liberdades de expressão para não ferir a outros direitos fundamentais alheios.

A prezada Segurança Jurídica é princípio básico assegurado na Carta Magna de 1988 e fundamento para a consolidação do Estado no meio real-virtual. Ela é um princípio que o Estado

tem que garantir, ao seu cidadão, uma certeza de que seus direitos serão devidamente resguardados e quando atingidos (até pelo próprio Estado), de que serão devidamente compensados. Por isto, trazemos a preocupação com a limitação e fiscalização da tutela e regulamentação do Estado. Assim sendo, nasce essa Segurança Jurídica para garantir aos cidadãos os seus direitos naturais fundamentais como o direito à liberdade, à vida e à propriedade. Para que uma norma possa ser perfeitamente aplicada em nossa legislação, é essencial que ela traga segurança ao ordenamento jurídico. Ou seja, esse fundamento está relacionado ao Estado defensor de direitos porque não é possível dar-se credibilidade a um ordenamento que está sempre sofrendo modificações, sem se preocupar com o próprio povo, devendo sempre prezar pela estabilidade e equilíbrio.

Para que haja a efetiva segurança jurídica, não pode o julgador exceder o que não fora permitido pelo legislador. Este direito fundamental do cidadão implica em normalidade, estabilidade e proteção contra alterações desproporcionais da lei. Devendo o Estado ter comportamentos coerentes, estáveis e não contraditórios. A previsão constitucional da segurança jurídica se encontra no art. 5º, XXXVI, da CF, onde dita que “a lei não prejudicará o direito adquirido, o ato jurídico perfeito e a coisa julgada” (BRASIL, 1988), denominadas estas últimas de Trilogia da Segurança Jurídica. Também podemos observar a Segurança Jurídica, em maior ou menor medida e de forma implícita ou explícita, em outras normas. Resumindo, podemos conceituar segurança jurídica como a garantia da exigibilidade de direito certo, estável, previsível, justificado e motivado com vistas à realização da justiça, devendo ser respeitada plenamente no combate aos cibercrimes.

A questão é até que ponto que a Segurança Jurídica não serve de justificação para o já visto Estado de Exceção Permanente? Não há fórmula secreta para isto e certamente a justificação de medidas totalitárias sempre encontrarão seus bodes expiatórios, na denominação que estiver na moda à época. E não por isto deve ser refutada, mas passível de críticas e observação caso a caso. Portanto, problemas de colisões de direitos e princípios de privacidade, liberdade de expressão, tutela da averiguação de informações e segurança jurídica sempre existirão. Qualquer possível solução, como a trazida por Alexy, será subjetiva: ou permite o engessamento deles, fazendo com que quase sempre um princípio prevaleça sobre outro ou permita a possibilidade caso a caso de um ser mais importante naquele contexto que outro. Não há outra escolha e qualquer uma dessas gerará problemas frutos da subjetividade humana. A questão é o como fazer estas ponderações. Sugerimos, desde então, que seja feito no mais específico caso a caso e que, caso a população não se sinta confortável, os juristas tenham a sensibilidade não automatizada e técnica, que lhe é imposto a sê-lo, de barrar estas intervenções

na vida humana. Ou seja, qualquer solução dada por qualquer outro autor que poderíamos expor aqui seria subjetiva, apenas citamos algumas possibilidades. Só é possível saber dos seus benefícios depois de aplicá-las. Assim, que o jurista tenha a sensibilidade de reconhecer quando errou, não atrelando tal técnica à sua personalidade ou ideologia política, e de sempre proteger os interesses coletivos e sociais.

### **3.1.1 Dinamismo dos direitos humanos fundamentais na rede**

*O Direito deve oferecer instrumentos jurídicos de efetivação dos direitos humanos fundamentais que se apresentem compassados.*

A definição dos direitos humanos foi e é um processo de reconstrução permanente, cumulativa e qualitativa (BONAVIDES, 2008, p. 517). O catálogo dos direitos humanos fundamentais não apresenta um conteúdo definitivo, mas são construídos pela humanidade no decorrer da história. Por exemplo, o cenário de desfecho da Segunda Guerra Mundial ensejou a necessidade de reconhecimento e respeito internacional dos direitos humanos, como na Declaração Universal dos Direitos Humanos de 1948. Atualmente, exige-se o reconhecimento pelo Estado de direitos que protegem os interesses do gênero humano e de toda a sociedade (transindividuais): o direito ao desenvolvimento, à paz, à autodeterminação dos povos, ao meio ambiente, à proteção do patrimônio comum da humanidade, à proteção do consumidor e à comunicação. São os denominados direitos de terceira geração ou dimensão (BONAVIDES, 2008, p. 569). Mesmo assim, a ideia de geração de direitos não significa a substituição de direitos, podendo ocorrer a redefinição de direitos e o reconhecimento de outros. Os direitos de determinada geração ou dimensão não são suprimidos com o reconhecimento de gerações posteriores, ao contrário, se somam e se complementam, constituindo o sistema jurídico do Estado Democrático de Direito (BONAVIDES, 2008, p. 572), sem obedecer a uma ordem cronológica absoluta.

Paralelamente à noção de autodeterminação dos povos, existe hoje uma preocupação com a coleta e tratamento de dados por provedores de internet em contraste ao exercício do direito à autodeterminação informativa. Como são diversas as cláusulas nos contratos de adesão destes provedores que permitem quase tudo a ser feito com seus dados pessoais, é praticamente nulo o controle informacional dos usuários, inclusive impedindo seus direitos básicos de se

autodeterminarem e de não serem subconscientemente determinados por empresas e IAs de propaganda direcionada.

Dessa mesma forma, o conceito de dignidade da pessoa humana se modifica no tempo e no espaço. O reconhecimento das quatro gerações demonstra este dinamismo histórico. Outra corrente da teoria dos direitos humanos classifica como direitos de quarta geração aqueles ligados ao direito à vida e aos desafios das novas tecnologias referentes à biotecnologia, bioética e engenharia genética, como manipulação do genótipo dos seres, patrimônio genético e abuso de técnicas de clonagem. Já os direitos da quinta geração surgem com o avanço da cibernética, advindos, portanto, das tecnologias da informação e da comunicação, da realidade real-virtual, do uso da internet e do ciberespaço (WOLKMER, 2012, p. 27-31).

Rui Viana e Cíntia Lima (2014) citam a fusão da figura do direito de personalidade a uma só expressão: vida privada (diferente de intimidade). A infração a este direito se dá através de hackers e *cookies* por exemplo, pela afronta à vida privada do indivíduo. Ela encontra-se também nas relações normais cotidianas entre particulares, geralmente na exposição não-consentida da esfera privada a conhecimento de terceiros, onde todo ato o qual excede o estipulado contratualmente, como na internet, merece uma ação judiciária para inibi-lo. Cita-se o caso do Direito ao Esquecimento, ainda não devidamente consolidado legislativamente, salvo casos de notoriedade pública e sinônimos afins.

Sobre o Direito à Imagem, o titular deste direito pode utilizá-lo para tirar proveito econômico, todavia, quando não há este consentimento ou se ultrapassa os limites autorizados, ocorre a violação da honra, sendo cabível a indenização por danos morais e materiais, salvo as particularidades dos casos de notoriedade, cargo público, fins científicos ou culturais e fatos de interesse público. A grande dificuldade na recomposição deste direito (o que chamamos de Eternalização de Condutas e Irreversibilidade do Dano) pode legitimar, na visão do julgador, um privilégio do interesse “mais importante para a ordem jurídica” – de quem teve a vida privada ofendida – em detrimento do menos importante, como por exemplo o da liberdade da informação, já que uma lesão ao direito da personalidade seria maior (VIANA; LIMA, 2014).

Ao tratar da tutela dos direitos da personalidade, a previsão de reparação pelo violador – com um *quantum* indenizatório apropriado – é um progresso histórico por causa da crescente preocupação com a vida privada do indivíduo. Na Alemanha e em outros países europeus, a tutela ao direito pode ser realizada de forma preventiva, pois após consumada a lesão, não há que se falar em perfeita tutela jurídica por se tratarem de direitos de conteúdo e função não patrimonial. A importância é tamanha que alguns autores relatam que sem proteção prévia, não há nem que se falar em direitos da personalidade. Afinal, a tutela preventiva busca proteger

justamente bens infungíveis. E ainda é ressaltada a importância do poder de *imperium* – e não só a previsão legal – para a devida ordenação da abstenção de certos atos aplicando medidas coercitivas adequadas de ordem efetiva, havendo até a possibilidade de antecipação de tutela inibitória com possibilidade de ser fungível, moldando-se assim à situação jurídica material. Nos Estados Unidos, assemelha-se às *injunctions* (VIANA; LIMA, 2014).

A irreversibilidade não pode ser um dogma em casos extremos, afinal é “melhor se conceder tutela capaz de evitar um grande prejuízo ao suplicante, mesmo com base na produção da ‘prova possível’ do que lhe denegar a justiça” (VIANA; LIMA, 2014). Portanto, a tutela inibitória, carente ao ordenamento jurídico brasileiro, apresenta três condições – uma positiva e duas negativas – e, assim, não visa prevenção imediata do dano (consequência), mas sim do ilícito. Vejamos que antes dos meios de comunicação em massa, a norma é a premissa maior, os fatos são a premissa menor e a conclusão (através da função técnica do juiz) é a consequência do enquadramento do fato à norma. Mas depois, há mais de uma premissa maior (mais de um direito tutelado do mesmo fato) e um só fato como premissa menor, impossibilitando a conclusão, devendo-se imputar a função de criação ao juiz, o que se chamou de ponderação, basicamente a razão de existir jurisprudência. Ao compreender a inaptidão dos critérios tradicionais para solucionar fatos complexos e plurais, a Ponderação – através de cláusulas abertas, conceitos indeterminados, princípios e princípio da proporcionalidade ou razoabilidade – transferiu, assim, essa competência decisória para o intérprete estipular à medida que um direito deve sobrepor-se a outro, nunca totalmente excludente e sempre preservando o máximo de cada. Assim, podem haver “normas constitucionais em tese, mas inconstitucionais em concreto”, à vista das peculiaridades do caso, com a ponderação sendo a solução (BARROSO, 2007).

Há duas características dos direitos da personalidade, eles oponíveis à toda coletividade e ao Estado (*erga omnes*) e nem sempre a violação tem repercussões econômicas. É feita a já consolidada ressalva de que aos notórios públicos – de alto grau de exposição pública – o interesse público é presumido, com redução do âmbito de proteção do direito, não chegando, porém, à supressão. Fora exceções, como o fato verdadeiro que é íntimo e segredo alheio, o direito à honra é limitado pela circunstância do fato ser verdadeiro e obtido por meios lícitos, como o de informações criminais, vide o famoso caso alemão Lebach (GERMANY, 1999). O Direito à Imagem protege a representação do corpo humano que depende dos limites da autorização do titular. As distinções entre liberdades de informação, de expressão e de imprensa (todos podem ser chamados “de comunicação”) não são tão relevantes à lei e à solução das colisões. Elas fundamentam o exercício de outras liberdades, ganhando assim uma *preferred*

*position*, mas não sendo direitos absolutos. Em nosso contexto globalizado e de multi-interesses, o interesse público na divulgação de informações é presumido. Estipula-se os parâmetros para ponderação da colisão: veracidade do fato, com a devida razoabilidade e boa-fé; licitude do meio de obtenção da informação; personalidade pública, como exceção; local do fato, em locais privados tem que haver autorização ou vontade dos envolvidos; natureza do fato, crimes, desastres naturais e acidentes não precisam de autorização das partes; existência de interesse público, este é mais relativo e inútil já que hoje em dia com as revistas de fofoca, toda informação se transforma presumidamente consumível e de interesse público; interesse público em fatos de órgãos públicos, entram na exceção de atores públicos; e preferência por sanções *a posteriori*, pouco aplicável às colisões pois esperar o dano pode “não ter reparação capaz de desfazer efetivamente o mal causado” (BARROSO, 2007).

Em uma acepção histórica, os direitos de quarta e quinta geração almejam proteger o ser humano face ao avanço tecnicocientífico. O que é importante notarmos, pois é justamente a adaptação jurídica a estes avanços que buscamos entender para sugerir mudanças. Sarlet (2010) afirma que as classificações de uma quarta e uma quinta dimensão são desnecessárias porque a quarta trata sobre a bioética, portanto, sobre a vida, já tutelada pela primeira dimensão de direitos humanos; e a quinta trata a respeito da cibernética e da informação, temas condizentes com a terceira dimensão de direitos. De qualquer maneira, o Direito deve ser repensado em razão da indeterminação das possibilidades tecnológicas, com a devida cautela para que esses não sejam relegados à condição de meras disposições programáticas ou políticas públicas.

No contexto da internet, o meio ambiente cibernético modifica as relações sociais e a formação cultural do ser humano. Por exemplo, a questão do monitoramento estatal e interpessoal começa ainda no berço, com as babás-eletrônicas, e estende-se por toda a vida adulta, por meio de câmeras de segurança (chamadas de CCTV). Na educação de crianças, vemos que, ao invés de brincadeiras ao ar livre, elas optam cada vez mais por videogames, celulares e até bichos de estimação virtuais. Crianças são cada vez mais condicionadas a reagir e não a refletir. Adultos, estejam na faculdade, na academia, num restaurante ou mesmo num piquenique no parque, estarão provavelmente utilizando um *gadget* ou app que permita a conexão com o ciberespaço, a todo momento os monitorando e, muitas vezes, ferindo sua privacidade.

O Brasil foi precursor no reconhecimento do meio ambiente artificial e no reconhecimento dos direitos humanos influenciados pelas inovações tecnológicas, como se verifica no Marco Civil da Internet e na inserção do direito de acesso à internet e do direito à

banda larga como direitos humanos fundamentais. No entanto, como já dito durante o trabalho, nota-se a insuficiência da análise das especificidades da sociedade contemporânea também pelo legislador, como na superficialidade de regulamentação do teletrabalho, que equipara o trabalho realizado no estabelecimento do empregador àquele realizado à distância, omissiva no que se refere às condições de trabalho, como no Direito à Desconexão. Tanto que as redes sociais têm substituído os sindicatos e associações. Sendo a plataforma de “voz do povo”, inclusive servindo para denunciar empresas que abusam dos consumidores. Mesmo com estas novas formas de adaptação social, o Direito deve oferecer novos instrumentos jurídicos de efetivação dos direitos humanos fundamentais.

Vejamos que a luta contra o ciberterrorismo, ao reclamar maior segurança, possui o preço da violação do direito de privacidade. O Estado tem buscado meios legítimos de atuação policial no combate e na prevenção da criminalidade, mas, como bem já vimos, pode servir a legitimar também um Estado de exceção permanente. Tem que haver algum tipo de limite. A atuação administrativamente eficiente do Estado e a prevenção do risco social não podem ser pressupostos irrefutáveis de conhecer o maior número de informações a respeito da sua população. Muitas vezes essa busca de informações é feita por entes privados com financiamento do próprio Estado. Portanto, devemos ser críticos com esta atuação estatal.

### **3.1.2 Tratamento de Dados Pessoais**

*Ninguém sabe o que é efetivamente feito com os dados.*

Qual real alternativa tem o usuário ao confiar a empresas ou organizações governamentais seus dados pessoais? A solução seria migrarmos para outros provedores ou entregarmos menos dados? Mas e se necessários para melhor controle e melhores políticas públicas? Quando há um limite para o poder justificado? A realidade mostra que o indivíduo é refém do formidável sistema técnico que controla a sua existência abrangendo uma rede de empresas, instituições e Estados. E, como vimos, o progresso técnico implica a perda da liberdade do indivíduo. Uma resposta razoável dos operadores do direito seria resistir ao sistema, desenvolvendo um controle democrático dos bancos de dados. Por exemplo, para cumprir esse rol no direito comparado, há as denominadas Comissões de Controle. Há também o controle interno de corregedorias e a *accountability*. De qualquer maneira, estaria em jogo o paradoxo do Estado controlando o próprio Estado, com os perigos de manipulações de poder e

de trocas de favores nestes sistemas. Mesmo que houvesse controle externo, digamos por um órgão privado, com uma eficiência dependente de caso a caso, há sempre o perigo dessa corrupção. Por outro lado, é necessário utilizar o Direito, não como mera técnica de controle a serviço do Estado, mas como último obstáculo da técnica informática que se impõe ao preço da liberdade e da violação do direito à intimidade das pessoas.

O direito à privacidade é altamente desenvolvido no direito europeu, especialmente pela Convenção Europeia dos Direitos do Homem (CEDH) de 1950. O artigo 8º da Convenção prevê o direito ao respeito pela vida privada e familiar, do seu domicílio e da sua correspondência, de importância tal que o Tribunal Europeu dos Direitos Humanos levou à Diretiva 95/46/CE de 1995 que regulava o tratamento de dados pessoais. Posteriormente, ela foi revogada e substituída pelo Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Segundo a GDPR, o titular dos dados tem direito de acesso a todos os dados sobre ele processados e pode exigir retificação, apagamento ou bloqueio dos dados que são imprecisos, vide o Direito de Esquecimento. Além disso, o processamento de dados só pode ser feito em três condições: transparência, finalidade legítima e proporcionalidade. Segundo o princípio da transparência, o titular dos dados tem o direito de ser informado como seus dados pessoais estão sendo processados; segundo a finalidade legítima, eles só podem ser processados para fins explícitos, legítimos e especificados compatíveis com essas finalidades; e segundo o princípio da proporcionalidade, eles só podem ser processados na medida de sua pertinência. Assim, os dados devem ser exatos e aqueles inexatos ou incompletos devem ser apagados ou retificados. E o titular pode opor-se a qualquer momento ao processamento de seus dados para fins de marketing direto, o que empresas fazem bastante. Você, leitor, já pesquisou algo no Google e, logo depois, foi encharcado com várias propagandas de produtos similares? Chega ao ponto que pessoas relatam que pensam em algo e este aparece a elas em propagandas. Teria a IA chegado a este ponto? De acordo com a LGPD, restrições adicionais devem ser aplicadas pelo menos no processamento de dados pessoais considerados sensíveis, aqueles referentes a crenças religiosas, opiniões políticas, saúde, orientação sexual, raça e filiações.

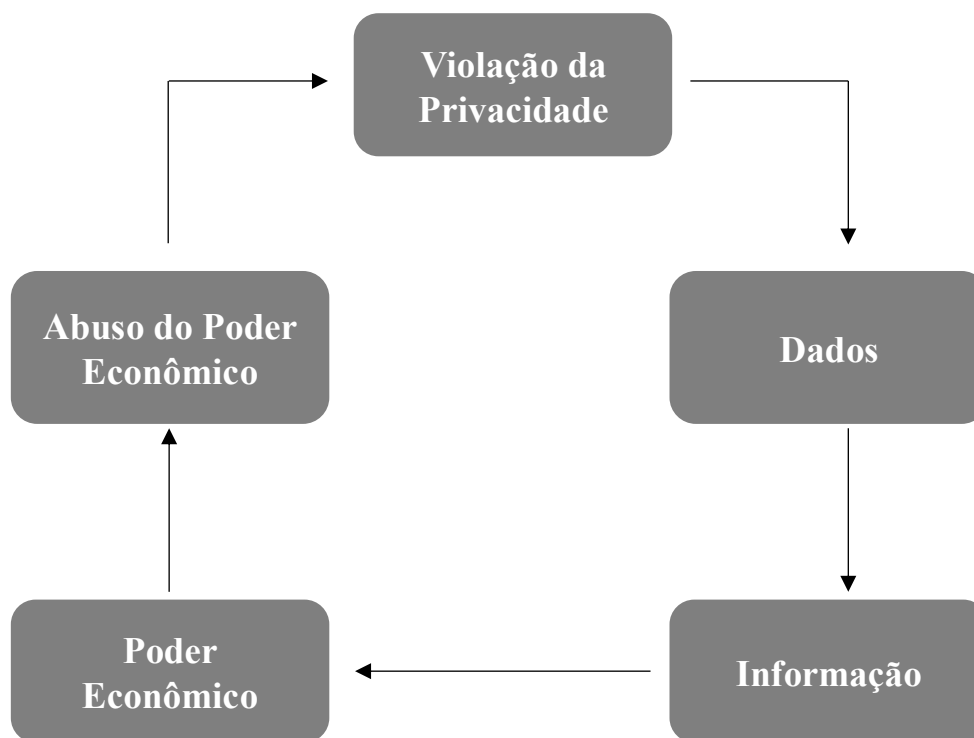
Já no Brasil, a Lei n. 12.965/2014, conhecida como Marco Civil da Internet (MCI), não é uma lei geral de proteção de dados pessoais. Ela não trata de todas dimensões deste tema, como a transferência internacional de dados, vazamentos de dados e dados anonimizados. Na verdade, é a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709 de 2018, a legislação brasileira que regula as atividades de tratamento de dados pessoais. Esta legislação se fundamenta em diversos valores, como o respeito: à privacidade, à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião, à

inviolabilidade da intimidade, da honra e da imagem, ao desenvolvimento econômico e tecnológico e a inovação, à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos liberdade e à dignidade das pessoas. Seu texto determina que todos os dados pessoais (informação relacionada à pessoa natural identificada ou identificável, como nome, idade e estado civil) só podem ser coletados mediante o consentimento do titular. Tratamentos de dados pessoais sem o consentimento do titular só ocorrem nas hipóteses específicas no art. 11, inciso II. No art. 18, a LGPD traz os direitos dos titulares de dados pessoais de: confirmação da existência de tratamento, acesso aos seus dados, correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a LGPD, portabilidade dos dados a outro fornecedor de serviço ou produto, eliminação dos dados pessoais tratados, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, revogação do consentimento e revisão por pessoa natural de decisões automatizadas. Por fim, as sanções administrativas para o descumprimento da LGPD estão no art. 52 e são elas a: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% do faturamento líquido da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada a R\$ 50 milhões por infração; multa diária; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais envolvidos na infração até a sua regularização; e eliminação dos dados pessoais envolvidos na infração.

O que nos interessa aqui não é uma análise jurisprudencial no Brasil. Nos interessa os problemas mais profundos e inerentes no tratamento de dados que advém da técnica. A primeira questão é a vigilância exacerbada do Estado. Vivemos o caso relatado de Snowden sobre a NSA americana, mas este é só um exemplo do efeito *Big Brother*. A China, por exemplo, já está realizando um banco de dados de dados faciais dos seus cidadãos e avaliando os mesmos por uma nota, ao estilo do episódio “Queda Livre” (2016) da série britânica “Black Mirror”. Quando trabalhamos esta questão, concluímos a necessidade de algum limite para as ações estatais porque a Segurança Jurídica como inesgotável fonte de um constante estado de exceção não pode acontecer. No mínimo, os Estados devem certa satisfação aos cidadãos, como após utilizar e violar certo dado pessoal sem a permissão prévia do usuário, deveria avisá-lo o como, quais dados e porquê fê-lo, para que o cidadão que sinta que foi violado desnecessariamente possa ser indenizado. Logo, criando uma certa limitação e jurisprudência sobre o tratamento de dados pessoais pelo Estado.

Outro problema que ocorre neste tratamento de dados por Estados, empresas ou indivíduos com alguma expertise computacional é o ciclo vicioso destas violações (Quadro 03):

Quadro 03 – Ciclo vicioso da violação da privacidade de dados pessoais.



(Fonte: TEPEDINO; FRAZÃO; OLIVA, 2019)

Alguns atribuem este ciclo que se retroalimenta ao capitalismo (ZUBOFF, 2019, p. 8), outros liberais-otimistas à natureza humana abstraída pelo mercado. É interessante notar que estes dados nos definem e nos representam, são como as empresas e Estados nos observam quantitativa e qualitativamente, ao mesmo tempo que ditam quem seremos, com suas previsões por padrões cada vez mais detalhadas. Estes dados nunca corresponderão a uma descrição objetiva do mundo, sendo sempre parciais e enviesados, no máximo são próximos da realidade. Por exemplo, uma pesquisa notou que a inteligência artificial de um hospital era “racista” ao sempre dar classificações de risco mais baixas a negros simplesmente pela cor de pele, logo, eles tinham menor probabilidade de serem encaminhados para programas que fornecem atendimento mais especializado quando estivessem tão quão doentes quanto pessoas de outra cor. Assim, negros tinham que estar mais doentes – quando, na verdade, são mais propensos a terem mais certas doenças como diabetes, anemia, insuficiência renal e pressão alta – do que os brancos para serem encaminhados para cuidados especializados (OBERMEYER *et al.*, 2019). Chega ao ponto da Cambridge Analytica, onde dados podem até comprar ou influenciar a

opinião pública durante uma eleição política (CONFESSORE, 2018). Outro exemplo é o das companhias de crédito, estatais ou privadas, que atribuem mais créditos a mais ricos e crédito mínimo irrisório a mais pobres, levando a maiores desigualdades. Afinal, como pode o pobre ter qualquer chance de evoluir economicamente com mais este degrau. Liberais defendem que estas dificuldades são naturais, mas coincidentemente há sempre mais e mais degraus para quem quer “subir na vida” e quando se soma todos estes degraus, eles perpassam por várias gerações. Assim, não pode o Estado esperar esta “natural escalada” e uma suposta igualdade de oportunidades que leva séculos sem mínima interferência estatal. Isto também vale para os dados onde o Direito não pode esperar que os Estados e empresas utilizem estes dados da maneira que bem lhes convier esperando que as vontades sociais sejam naturalmente abstraídas pelo mercado traduzindo na tendência de oferta-demanda para que as empresas tratem melhor os dados; até porque são pouquíssimas as maiores empresas e não há tanta concorrência.

E o que queremos dizer com todas essas críticas? Que acabem os dados pessoais e sensíveis? Não. Dados pessoais e sensíveis, mesmo que houvesse uma proibição absoluta de todos Estados, jamais deixariam de existir. Eles são fonte primária de algoritmos e provedores para poderem minimamente atuar. São necessários para o funcionamento da rede. Já vimos e ainda veremos que não há como ser contrário a estas ou a qualquer tecnologia, mas tão somente opinarmos sobre e/ou restringirmos seu uso e sua forma de utilização, neste caso o tratamento. Mostramos que o mal-uso dos dados pessoais – assim como de qualquer tecnologia – é culpa da ambivalência da técnica. E como se lida com esta ambivalência? Na internet, nos parece que a melhor maneira é agir após identificar os problemas e utilizar o mínimo possível os dados. Mas como dito, é difícil inverter essa tendência. Por que empresas ou Estados extrairiam menos dados se são pequenos os malefícios (como possíveis *data breaches*) ou se não há nada que os impeça, já que não há como haver uma fiscalização detalhada dentro da própria empresa? Neste sentido, a atribuição específica do Encarregado de Proteção de Dados (Data Protection Officer – DPO), um funcionário da própria empresa que deve denunciá-la quando tratar mal dados, parece ser um grande desafio na lógica capitalista de maior lucro possível, cuja denúncia poderia atrapalhar, como vimos no subcapítulo “Insuficiência das Empresas”. Também vemos a dificuldade de *accountability* que terá a Agencia Nacional de Proteção de Dados (ANPD) no Brasil. Infelizmente a solução é ter mais técnica: uma maior fiscalização. De alguma forma, o povo e/ou o Estado precisariam ter uma ferramenta que o informe especifica e integralmente tudo que há sobre os mesmos e a forma e onde dados sobre os mesmos estão. Mas esta ferramenta não existe. E se existisse, traria outros problemas como seu mau uso por cibercriminosos para identificar as informações de certo alvo e as usarem em seu proveito. Não

há outra alternativa, senão aquela de sairmos completamente da internet, para lidar de maneira minimamente eficaz com o mal tratamento de dados, afinal a internet é completamente artificial e a solução seria também necessariamente. Chegamos ao ponto em que, pelas configurações do meio digital, ninguém – nem mesmo funcionários de um provedor – sabe o que é efetivamente feito com os dados. O aplicativo Uber, por exemplo, possui um histórico de abuso regular dos dados de localização dos seus usuários com uma espécie de “visão de Deus”, uma ferramenta que observa em tempo real de históricos de localização sem a permissão dos usuários.

Lembrando que há uma endêmica insegurança nos meios digitais já que o usuário tem muito pouco a fazer já que tais elementos estão fora de seu controle. Assim, a grande assimetria informacional existente entre as grandes empresas de tecnologia – conhecedoras das tecnologias que usam – e o consumidor, além da natural desigualdade econômica, causa sua hipossuficiência, potencializando sua vulnerabilidade (TEIXEIRA, 2007, p. 132). A sua hipervulnerabilidade relaciona-se com o alto conhecimento técnico que quase nenhum consumidor possui e se o mau uso ocorre em função da falta de compreensão – quase natural – desse meio eletrônico, não deve ser reconhecida a culpa exclusiva do consumidor nestas condições ou, pelo menos, deve ser levada em consideração.

Todas estas considerações são relevantes ao observarmos o direito fundamental a proteção de dados pessoais, bancos de dados e *big data*, desenvolvimento de leis de proteção de dados, princípios de proteção de dados e esta proteção no ordenamento brasileiro. Os bancos de dados proporcionam a extração do máximo de proveito possível e, independente da distinção entre dado e informação, eles possuem um poder absurdo. No panorama brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, mas da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade. Deve o Brasil reconhecer que estas garantias estão em risco com o tratamento atual dos dados pessoais especialmente porque, como bem diz Danilo Doneda (2014), e que este importantíssimo doutrinador de Direito Digital descanse em paz, não há consideração dos riscos objetivos potencializados pelo tratamento informatizado das informações pessoais por não abranger a complexidade do fenômeno da informação. Há um abismo que segrega a tutela da privacidade da tutela das informações pessoais em si, possibilitando a perigosa interpretação que pode eximir o aplicador e o provedor-julgador na utilização abusiva de dados dos usuários. Apenas reconhecendo a íntima ligação dos direitos relacionados à privacidade e à comunicação de dados, seria dado o passo necessário à integração da personalidade nas vicissitudes da sociedade técnica (DONEDA, 2014).

### 3.1.2.1 *Consentimento Quase-Tácito*

*Os usuários só estão conscientes que são desinformados.*

Qualquer tipo de tratamento pode ser feito desde que dentro das obrigações legais e sendo devidamente consentido e informado? O tratamento de dados traz diversos problemas legais. A Doutrina e a jurisprudência tentam acompanhar, assim como o legislador. O Marco Civil da Internet e a LGPD estabelecem ótimas formas de lidar com este tratamento e as tutelam de maneira satisfatória, deixando pouca margem para casos atípicos. Nossa indagação é, na suposição de que seja feito todo cumprimento legal, se mesmo assim se pode tudo no tratamento se consentido. Quando o consentimento não é mais lei? Qual o limite do tal consentimento informado e esclarecido, tão presente nos Termos de Contrato recorrentes na internet?

É difícil que empresas e Estados acatem as medidas jurídicas. Há a dificuldade de fiscalização, de efetivas denúncias, do usuário ter o conhecimento do mal tratamento e, ainda mais, ter provas de que teve o dado maltratado, como por exemplo saber qual foi o site que vazou a informação do seu e-mail a terceiro que envia *spams*, dentre os vários que compartilhou um mesmo dado. Outra dificuldade é a internacionalização destes dados. Lembrando que grande parte das pessoas já tiveram seus dados tratados indevidamente e provavelmente vazados em algum episódio de vulnerabilidade. Essas pessoas raramente têm conhecimento técnico suficiente para identificar esta vulnerabilidade, quem dirá para tomar uma decisão conjunta que abstraia uma vontade coletiva de, por exemplo, escolher outra rede social só por isso ou ter os meios econômicos e conhecimento técnico para se criar outra plataforma melhor. Tudo isso sem adentrar na questão de crianças e adolescentes.

Apesar de tudo isso e muitas outras dificuldades, suporemos que a empresa cumpra os deveres legais e obedeça aos requisitos para o tratamento através de um consentimento informado e esclarecido. Neste caso, quais são os limites desse consentimento? Tudo pode o usuário consentir quando clica no “Concordo”? Assim, voltamos a questionar, qual o limite do consentimento? A lei traz diversas ponderações, mas após haver o consentimento claro e aceito pelo usuário, parece não haver maiores obrigatoriedades, exceto o bom tratamento, questão subjetiva como os dados necessários devem ser bem tratados, que o período de armazenamento deve ser curto e o que o acesso aos dados deve ser limitado. A doutrina e a lei dão imensa preocupação, como devem, ao consentimento ser bem realizado, pois deve haver autonomia do usuário e a proteção ao mesmo, como não exceder a empresa àquilo pactuado com o usuário.

Todavia, parece não preocupar com o limite do consentimento. Por exemplo, se consentido através de imensos textos técnicos que se pode compartilhar seus dados para parceiros comerciais, deve então este compartilhamento ser realizado sem demais preocupações já que fora consentido? Independentemente do que empresas e Estados colocarem nos Termos de seus websites e aplicativos, tudo ali é lícito, válido e estimulável desde que o usuário aceite (tacitamente)? Trataremos de duas possibilidades de recusa.

A possibilidade de recusa é possível e “simples”, mas praticamente irrelevante pois com extrema raridade um usuário deixará de utilizar uma rede, provedor ou aplicativo por discordância aos termos. E se raramente o fará, não há no que se falar da “libertária liberdade” de escolha. Ela pode acontecer durante o tratamento: o usuário pode solicitar saber quais dados a empresa tem sobre ele e pode pedir para que excluam estes dados, desligando-se deste provedor em particular. Este desligamento é possível, mas dificilmente o usuário saberá com mínima certeza que teve seus dados apagados. Há evidências de que a formatação completa de um computador ainda assim não exclui uma série de dados que podem servir de objeto para uma investigação policial. Não há verdadeiras garantias no meio digital. É impossível que o usuário saiba, até porque quem oferecerá o relatório comprovando a exclusão dos dados é a própria empresa. E é ainda mais difícil – quase inexistente o contexto em – que o Estado dê esta autonomia ao indivíduo, dele escolher quais dados pode o Estado guardar sobre ele. Derivado deste mesmo problema temos o Direito ao Esquecimento, mais destinado a figuras públicas, mesmo que particulares possam solicitá-lo, onde o indivíduo quer que certos fatos de sua vida – que não são de interesse público – sejam apagados ou, no mínimo, irastreáveis pelos provedores de pesquisa como o Google. Um relatório completo sobre os dados que certa empresa tem sobre o indivíduo já é difícil de se obter, como veremos no seguinte subcapítulo “Término do Tratamento de Dados”.

Assim, o desligamento durante o uso já tem suas dificuldades, mas e a recusa antes do uso, a recusa ao se discordar dos Termos de uso? O usuário simplesmente não terá como utilizar aquele serviço. É um pacote quase sempre completo em que se recusa e não se usa o serviço ou o aceita e concorda tacitamente com todos termos. Neste segundo contexto que trazemos de recusa, raríssimas vezes há opções de concordâncias parciais e mesmo quando há esta hipótese, são pouquíssimas as opções dentro de tantos outros termos. Estes termos são parecidos com os Contratos de Adesão, referidos como *take-it-or-leave-it*, em que o aderente só pode aceitar o contrato tal como está ou rejeitá-lo, sem possibilidade de modificá-lo. De acordo com art. 51 do Código de Defesa do Consumidor (CDC), são vedadas disposições contratuais abusivas, tais como: cláusulas que impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor

por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos; cláusulas que subtraíam ao consumidor a opção de reembolso da quantia já paga, nos casos previstos neste código; cláusulas que transfiram responsabilidades a terceiros; cláusulas que estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada ou sejam incompatíveis com a boa-fé ou a equidade; cláusulas que deixem ao fornecedor a opção de concluir ou não o contrato, embora obrigando o consumidor; cláusulas que permitam ao fornecedor, direta ou indiretamente, variação do preço de maneira unilateral; e, por fim, cláusulas que autorizem o fornecedor a cancelar o contrato unilateralmente, sem que igual direito seja conferido ao consumidor. Ademais, há casos de abuso quando somente informam o conteúdo do contrato quando este já está aceito ou somente permitem baixá-lo quando o consumidor já se tornou contratante (MARQUES, 2004, p. 272).

Segundo Maria Helena Diniz (2006, p. 755), o contrato eletrônico “é uma modalidade de negócio à distância ou entre ausentes, efetivando-se via internet por meio de instrumento eletrônico, no qual está consignado o consenso das partes contratantes”. Apesar de não adentrarmos às suas classificações (como os contratos de adesão *click-wrap agreements* e *browse-wrap agreements* e os termos e condições de uso *shrink-wrap agreements*), todos são marcados por vantagens (simplificação do processo de contratação e eficiência econômica) e desvantagens (desequilíbrio entre as partes e consequente vulnerabilidade dos consumidores), características deste tipo contratual. Os contratos eletrônicos são diferentes dos contratos de adesão pois produzem desequilíbrio ainda maiores entre as partes contratuais, colocando os consumidores em posição de maior vulnerabilidade. De acordo com a professora Dra. Cíntia de Lima (2009, p. 347), essa desigualdade decorre da(o): complexidade técnica dos sistemas que efetivam as transações via rede, sobre os quais os usuários usualmente possuem conhecimentos limitados, ao passo que os fornecedores são profissionais com conhecimentos especializados; fornecimento de informações incompletas ao consumidor sobre o produto ou serviço que está sendo transacionado; e limitações impostas à privacidade do usuário para que lhe seja permitido transacionar com os fornecedores, sendo frequentemente necessário que aqueles cedam a estes uma grande quantidade de dados pessoais. Ou seja, os contratos eletrônicos propiciam eficientemente e com baixo custo produtos e serviços, mas ao mesmo tempo há redução do acesso a informações claras, aumento da complexidade das transações – levando à desinformação pelo consumidor – e a consequente diminuição de sua privacidade e segurança.

Em todo o mundo e não só no Brasil, parece ainda não haver entendimento, jurisprudência e nem mesmo direcionamento doutrinário sobre o que poderiam ser as “cláusulas

abusivas” no contrato eletrônico e quando há, são genéricas sem mostrar no caso concreto como empresas e Estados podem abusar desta espécie contratual. E em menos cenários, Estados atuam contra estes abusos empresariais. Há cinco características marcantes destes contratos que geram consequências ruins aos consumidores, Orlando Gomes (1972, p. 88) elenca a: unidade e invariabilidade, afinal o contrato é único para todos consumidores sem personalização alguma e falta de opções quase nunca é um bom indício de que os direitos ali serão otimizados e protegidos o máximo possível; a complexidade e tecnicismo, porque a complexidade destes contratos quase nunca será conhecida pelo consumidor e o não desconhecimento de lei ou de contrato devidamente assinado não podem ser motivos de reclamação ou justificativas de abuso; generalidade ou permanência da oferta, como estes serviços estão geralmente dispostos a todos e custa quase nada que haja mais consumidores destes serviços virtuais, eles estão sempre disponíveis e facilmente aderíveis; superioridade ou prepotência econômica, o que pode um consumidor fazer se discordar de certo contrato, simplesmente não utilizar e comprar aquele serviço, se não aderir a outro serviço semelhante ou criar um outro; e o estado de necessidade, geralmente o consumidor nem lê o termo e já o aceita porque ele precisa – não no sentido de sobrevivência física, mas sim social.

Mesmo que cláusulas contratuais sejam interpretadas favoravelmente ao consumidor (art. 47, CDC) ou haja o reconhecimento da sua vulnerabilidade (art. 4º, inciso I, Lei n. 9.008/1995), os problemas elencados não desaparecem. A sanção do Código de Defesa do Consumidor foi criada para coibir as cláusulas abusivas, mesmo que a nulidade de uma cláusula não extinga o contrato, salvo no caso de grande prejuízo para ambas às partes em que o aderente não precisa aguardar a sentença para deixar de cumprir esta. Mesmo assim, na maioria dos casos na internet, o consumidor quer – por uma necessidade social artificialmente criada – adquirir o produto ou o serviço em questão e ele não possui conhecimento técnico, ficando vulnerável e hipossuficiente.

Constatemos: como participar de qualquer outra rede social se não as redes do Facebook, Instagram ou WhatsApp? Aliás, todas estas maiores redes são de uma única empresa, a Meta. Poderíamos incluir outras redes, como o TikTok e mesmo assim, as opções demonstram-se escassas. Se o indivíduo escolhe não utilizá-las, se isolará quase completamente, pois a maioria permanecerá nelas. Observando o Facebook e o Instagram ou qualquer outra rede futura que as desbanque e venha a viralizar: não há tantas opções assim se considerarmos ser mais proveitoso estar em redes em que a maioria está. Aplicativos e sites de comunicação são mais fáceis de variar como o WhatsApp ou Telegram, mas mesmo assim é complicado abandoná-las pois um outro interessado teria que ter esta mesma alternativa e, mesmo tendo, a maioria

continuará nestas principais. Há outros tipos de serviços como de endereços e mensagens eletrônicas como Hotmail (Microsoft), Yahoo e Gmail (Google) ou serviços de nuvem como OneDrive, GoogleDrive e iCloud. Nestes casos, também é complicada a escolha e confiança em outras alternativas, além da dificuldade de outras plataformas deste tipo existirem pois a guarda massiva de dados demanda investimentos milionários.

Outro problema é a questão da “necessidade”. Ninguém precisa estar na rede, é possível (sobre)viver sem se comunicar com ninguém até pessoalmente, quem dirá virtualmente. Mas na realidade em que temos que trabalhar por exemplo, há muito tempo temos a necessidade de comunicação – virtual – e de dar importância à imagem/simbolização. Mediante a necessidade social de comunicação virtual – não é por isso que a maioria tem celular, utiliza as redes sociais e comunica-se por aplicativos? –, há sim uma necessidade coletiva abusada por entes que detém o poder sobre o meio destas comunicações.

Numa visão liberal, o mercado agiria contra as *data breaches* ou ataques às suas vulnerabilidades, mas, exceto algumas baixas em bolsas de valores, estas empresas conjuntamente perdem poucos consumidores. O mercado deveria reagir criando empresas para competir, como bem aconteceu no caso do Facebook em sua época, superando aqui no Brasil o Orkut ou como o WhatsApp fez ao superar o Windows Live Messenger (MSN), que anteriormente já havia superado as mensagens das operadoras via SMS. Mas estes processos são morosos, deixando os dados à mercê do provedor ruim enquanto não é viralizado outro do tipo, e quando há uma mudança de rede social ou provedor de e-mail ou de nuvem mais utilizados, outros poucos, geralmente no máximo cinco da mesma categoria para cada país, serão criados e tomarão conta, permanecendo o problema ainda: as cláusulas desnecessariamente abusivas de contratos de alguns imensos provedores de serviços na internet. Mesmo que haja morosamente – geralmente de três a quinze anos atualmente para que uma rede bem consolidada seja conquistada por outra – a superação, ainda serão pouquíssimas e poderosas as empresas; troca-se as empresas, mas não a hipossuficiência do usuário.

Assim sendo, mesmo no ideal mais liberal – que não existe, pois, a perfeição do mercado é um ideal – o problema não é solucionado. Demanda-se um conhecimento técnico e investimento inicial tais que a oferta de serviços não é grande suficiente para que o mercado consiga mitigar o abuso. Estes serviços demandam adesões coletivas muito grandes, gerando certas monopolizações difíceis de serem superadas e mesmo quando são, os mesmos problemas e o mal manejo de dados permanecem. Então qual a solução? Não buscamos difamar empresas do ramo digital, tampouco empresas em geral. A empresa e o empresário não são lobos que retiram maquiavelicamente a mão-de-obra do povo. A mais-valia existe, assim como a

alienação pelo trabalho, mas não há ainda melhor alternativa e estes geram seus benefícios, individuais e coletivos. Este tipo de serviço demanda conhecimentos muito específicos e geralmente começam com poucas pessoas que colocam uma ideia em prática. A ideia do empresário como mau é ultrapassada. Vimos que o empresário é também uma outra vítima do “querer mais eficiência”. O empresário é, muitas vezes, alguém que já foi um trabalhador explorado. Ele está em uma posição superior e deve pagar por seus abusos, mas não deve ser desonrado apenas por sê-lo. Devemos enaltecer a criatividade humana e a iniciativa privada, com todos seus benefícios. Não há sentido em soluções que sugerem uma exclusão de empresas ou de qualquer iniciativa criativa das pessoas, como se sua suposta antítese fosse um socialismo ou comunismo. O problema também não é o lucro em si. Objetivamente, as empresas exploram os dados pessoais a mais do que deveriam porque querem lucrar. Mas o problema não é o lucro, pois é só uma representação, um meio como qualquer outro, “a moeda da vez”, que poderia ser tratado como representação das vontades particulares, mensuração das atividades econômicas humanas, medidor da ambição humana quando colocada na prática (pela criação ou especialização), ao ter acesso aos meios possíveis (e aqui entrariam os problemas de igualdade de oportunidades por exemplo).

Independente desse meio técnico – o qual não trataremos da possibilidade de sua inexistência pois seria ilusório –, precisamos desses meios digitais e eles são fornecidos por poucos. É mérito dessas empresas criarem serviços bem personalizados, ajustados às demandas sociais e de mercado. Essas empresas têm mérito por terem conquistado o público. A questão também não é essa. O que propomos, portanto, mediante insuficiência e até falta de vontade empresarial de agir de forma diferente do “querer explorar monetariamente tudo ao seu dispor o máximo possível”, é alguma forma não de barrar, mas de controlar quando se trata dos dados pessoais. Controlar para proteger o usuário.

Primeiramente, temos a necessidade da tutela estatal como todo. Qualquer medida restritiva nesse sentido viria por controle externo realizado pela via administrativa, judicial ou legislativa. Em segundo lugar, o consentimento tem que ser expresso, claro e informado. As opções são limitadíssimas, sempre por contratos eletrônicos (de adesão) praticamente idênticos, permitindo que quase tudo seja feito – como compartilhamento para qualquer parceiro comercial – com estes dados, além da necessidade social de interagir através dessas redes, inclusive para trabalho e empregabilidade. Na verdade, não há verdadeiras escolhas. O usuário que quer permanecer conversando com seus amigos, interagir como qualquer ser humano, não tem a opção de sair; o usuário que precisa dessas plataformas para interagir com colegas até dentro do trabalho ou para se exporem para fins de empregos, também não têm

muito para onde fugir. Então, será que o consentimento que é expresso, claro e informado é verdadeiramente livre?

Essa aceitação do contrato pelo aderente pode ocorrer de modo tácito ou expresso. Aceitar tacitamente é agir em concordância com aquilo que é exigido no contrato sem que haja um documento escrito; e aceitar expressamente, é manifestar a concordância em documento escrito. Pelos motivos já elencados, o usuário nem lê a maioria dos contratos eletrônicos e se os lesse, não teria muitas opções para escapar, muito menos para escolher outros serviços em que as cláusulas não sejam igualmente abusivas. Ele nem tem conhecimento técnico para entender aqueles termos, quem dirá escolher. O usuário, na imensa maioria das vezes, então, não lendo ou discordando por pressão de mercado e da sociedade, realmente tem escolha? Qual a real utilidade desse consentimento? Parece não haver utilidade, exceto para o estabelecimento da relação contratual consumerista para o Direito. Se, na concordância-quase-tácita do usuário pode ocorrer abusos e cláusulas abusivas, por que não exigir, por exemplo, que os provedores (de *backbone*, acesso, hospedagem, conteúdo, informação, comércio ou correio eletrônico) não compartilhem esses dados de absolutamente nenhuma forma com terceiros? Que se crie uma categoria específica, por exemplo, de “provedor de conteúdo (ou propaganda) personalizado(a)” que tem como único objetivo divulgar seus dados pessoal para categorias de empresas e serviços que deseja. Qual é a utilidade para o usuário que suas informações sejam compartilhadas por parceiros comerciais sem querer especificamente isto? Não há uma verdadeira utilidade, a personalização de serviços e *ads* não compensa, a escolha pelo não-compartilhamento deveria ser a regra. Caso fosse vontade do consumidor, ele optaria pela exceção de querer uma personalização de serviços e *ads*. Com medidas inibitórias como essa, empresas teriam menos interesse de angariar mais dados do que precisaria para personalizar e memorizar o atendimento ao seu usuário-consumidor, levando até a menores prejuízos decorrentes das inevitáveis *data breaches*.

Juridicamente, o consentimento legitima o contrato, assegurando os direitos e deveres para aqueles contratantes, além de informá-los devidamente e isto é benéfico e bom. Mas é útil somente em pouquíssimos casos já que a maioria dos aplicativos já vem com estes contratos genéricos. O grande problema é o imenso foco que se dá para que o consentimento seja “expresso, claro e informado”, sendo que não resolve quase nenhum problema prático, ele só inicia um litígio ao demonstrar que ali havia certa relação de consumidor e sua falta não ensina necessariamente a inexistência de uma relação consumerista. São divagações jurídicas que não resolvem os problemas práticos do grande poder das poucas empresas e de suas autonomias desenfreadas para fazerem quase tudo com dados, especialmente se for

concordado pelo usuário porque não há como fiscalizar de dentro da empresa se há um devido cumprimento da lei. Se a maioria dos usuários nem leem os Termos, como podem eles ser informados? Os usuários só estão conscientes que são desinformados.

Liberalmente, se os usuários não importam é porque se trata de uma abstração da vontade coletiva, significando que, logo, não há o que preocupar. Tudo aquilo que não há uma coesão clara, objetiva e organizada da população não merece preocupação e, tampouco, influência estatal. Mas é absurdo que o Estado nada faça nestas situações. Guardada as devidas proporções, existem direitos que a pessoa não pode se desfazer mesmo se quisesse, muitos deles são os direitos de personalidade. Neste sentido de proteção ao indivíduo (até de si próprio), por não enxergar as consequências do fornecimento de seus dados quase tacitamente às empresas, é responsabilidade do Estado protegê-lo. Deixá-lo à mercê da boa vontade empresarial é imprudente e irresponsável. Não pode o Direito deixar a consequência devastadora do uso arbitrário dos dados pessoais, pelo consentimento quase-tácito, que temos hoje nos contratos eletrônicos. Já citamos alguns casos devastadores de *data breaches*.

Neste sentido, há respaldo internacional na interpretação da GDPR que faz com que seja possível: o processamento justo e legal de dados; o necessário consentimento do usuário para que suas informações sejam armazenadas; a especificação do propósito ou a finalidade do armazenamento, pelo responsável; a coleta mínima, estritamente necessária e limitada temporalmente de dados pessoais; a restrita divulgação de dados a terceiros; o controle da publicidade irrestrita aos dados; e a responsabilidade objetiva em relação à proteção dos bancos de dados por seus detentores. Ou seja, há duas preocupações majoritárias: a tutela na pertinência do armazenamento e o consenso do interessado. E como vimos, o consenso do interessado hoje é banal com quase todo aplicativo e *website* contendo um Contrato de Adesão genérico e quase todo usuário o aceitando sem ler, para que, em caso de eventual litígio, ele possa entrar na justiça a fim de garantir seus direitos. Portanto, parece ser mais importante a primeira preocupação: a tutela na pertinência do armazenamento, pois as empresas e Estados abusam da margem interpretativa e subjetiva do que seria esta pertinência. E não pode o Direito e o povo deixá-los tratar e utilizar seus dados sem nenhum limite palpável.

### **3.1.2.2 Término do Tratamento de Dados**

*O dado permanece na rede indefinitivamente.*

Sabe-se que a LGPD não impede o tratamento de dados: realizado por pessoa natural para fins exclusivamente particulares e não-econômicos; para fins jornalísticos e artísticos; para fins acadêmicos; realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão das infrações penais; e dos dados coletados, tratados e utilizados fora do território nacional. Sabe-se também que o MCI prevê a exclusão dos dados pessoais como um direito:

Art. 7º. O Acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...]

X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei. (BRASIL, 2014).

E o término do tratamento de dados foi regulamentado nos art. 15 e 16 da LGPD:

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:  
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;  
II - fim do período de tratamento;  
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou  
IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:  
I - cumprimento de obrigação legal ou regulatória pelo controlador;  
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;  
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou  
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2019).

Mas como podem a lei e o Estado garantir que a empresa ou um indivíduo encerrarão estes tratamentos, se desfazendo dos dados no tempo legal? E o dano feito pelo mal tratamento desses dados? O que podem o legislador ou o Estado ou o Direito fazer pelo dado pessoal que já lançado na internet? Deve-se, por isto, considerar a atividade de tratamento de dados sempre de risco ou só no caso de dados sensíveis? Essas perguntas são as que verdadeiramente importam ao lidar com o tema. O Direito ao Esquecimento é diferente desse término de tratamento, mas as dificuldades de fiscalização do cumprimento desses direitos são os mesmos.

Como bem vimos durante esta dissertação, as características da técnica e da tecnologia geram estes problemas, cada uma em sua dimensão. A Irreversibilidade Espaço-Temporal do Dano e a Eternalização de Conteúdo Digital geram consequências irreparáveis. Nenhum dano

é completamente reparável, pois perde-se o tempo e lugar em que aquele mesmo objeto ou serviço encontravam-se e a indenização é a forma prática de tentar abstrair monetariamente a extensão e gravidade do dano. Logo a natural irreparabilidade é solucionada – pelo menos, juridicamente – pela indenização por danos morais e materiais, mas o dado permanece na rede indefinitivamente. Não há meio conhecido hoje de se identificar, através de uma chave-mestra, o compilado de qualquer informação ou dado da internet, há menor ainda possibilidade de se retirar este suposto compilado. É por esta gravidade e particularidade do mundo real-virtual em relação ao tratamento, que devem todos entes do ciberespaço buscar o mínimo possível de informações do usuário, mesmo que deixe de lucrar ainda mais ao guardar somente os dados necessários, até por estes serem requisitados pelo MCI e pela LGPD.

Não se pode separar o perigo de um *data breach*, tampouco se pode retirar os dados da rede após lançados e prever os efeitos desses tratamentos. Na maioria das vezes o que se faz no Direito de Esquecimento é limitar os mecanismos de buscas, ou seja, retira-se os *links* do Google e outras ferramentas, fazendo com que o usuário não consiga pesquisar tal informação a qual um indivíduo queria que legitimamente seja esquecida. Os usuários só se dão conta da inexistência de proteção aos seus dados quando ocorre um evento danoso a sua privacidade. Assim, deve-se ter o maior número de cautelas nessa técnica de tratamento, colhendo o mínimo possível os dados, por empresas e Estados. Devem eles lidar com o tratamento como se realmente fosse sempre uma atividade de risco ou então as consequências serão nefastas.

Finalizando o tema de dados pessoais, citaremos uma das ações da Europa contra o Facebook, o emblemático Caso Schrems. O Tribunal de Justiça da União Europeia (TJ-UE) decidiu que as autoridades norte-americanas não garantiam a proteção dos dados europeus, invalidando um acordo de 2000. A decisão foi resposta à acusação de Schrems de que o Facebook violou as leis de proteção em vigor na Europa, defendendo que a transferência de dados para os EUA deveria ser reavaliada. Depois de várias queixas sobre as políticas de proteção da privacidade do Facebook, a Comissão de Proteção de Dados da Irlanda – país da filial do Facebook que controla as contas dos usuários, com exceção das contas de americanos e canadenses – exigiu que a rede social revisse algumas das suas condições quanto ao controle da privacidade pelos utilizadores e a possibilidade de desligar a função de reconhecimento facial do Facebook. Schrems considerou que a posição da comissão de proteção de dados irlandesa poderia ter sido mais firme e, por isso, apresentou uma contestação contra o Facebook a título individual no seu país, na Irlanda e no Tribunal de Justiça europeu. Durante este processo, criou a iniciativa *Europa vs. Facebook*, à qual aderiram dezenas de milhares de usuários. Condenou ainda a vigilância pelo Facebook através do botão “like”, bem como a

capacidade da rede social em analisar detalhadamente os seus membros através das interações dentro da rede social, exigindo uma atualização do sistema *Safe Harbour*. Outra das acusações foi o apoio da rede social ao programa PRISM, de monitorização e análise de dados dos serviços secretos dos EUA, denunciada a partir de documentos obtidos pelo Edward Snowden.

Depois de duas ações, nos anos 2015 e 2020, o Parlamento Europeu (EUROPEAN UNION, 2022) reforçou a necessidade de os governos assegurem que continuam a disponibilizar métodos confiáveis para transferências de dados e que resolvem qualquer questão relacionada com a segurança nacional, mostrando a tamanha dificuldade deste tipo de ação judicial. Este resultado de quatro anos de batalha simbolicamente teve resultado, mas na prática, até hoje, o Facebook por exemplo não mudou tanto sua forma de tratar dados com seu irretratável argumento de que não pode controlar o tratamento dos dados pessoais, pagando multas até quando puder, sem modificar comportamentos, semelhante à atitude da Apple sobre o fornecimento do método de desbloqueio de seus iPhones às autoridades investigativas americanas.

### **3.1.3 Busca e Apreensão sem Mandado Judicial**

*Todo ato criminoso pela internet é permanente.*

De acordo com nosso Código Penal, crime permanente é aquele de momento consumativo estendido temporalmente por domínio do criminoso acerca do momento de consumação do crime. Por exemplo, o crime de possuir pornografia infantil tem caráter permanente, assim como o de lavagem de dinheiro. E pelas características singulares da internet e alcance da conduta criminosa inclusive em nível internacional, ocorre esta incidência pois, majoritariamente, é um crime plurilocal e à distância. O grande benefício para o Inquérito Policial é a possibilidade da prisão em flagrante. Renato Lima (2013, p. 496) doutrina que crimes plurilocais são aqueles de cunho penal com ação e resultado ocorrendo em locais diferentes. Crimes à distância são infrações penais as quais acontecem dentro do Brasil, mas o resultado se materializa no estrangeiro ou vice-versa. Para tanto, a determinação da competência prevista no artigo 70 do CPP, em caso de crime permanente, estará firmada pela prevenção do art. 71 (CAPEZ, 2012, p. 277).

O crime permanente tem momento consumativo que se prolonga no tempo e a consumação continua ocorrendo enquanto perdurar o delito, como ao portar conteúdo digital ilícito, manter conteúdo postado em rede sem permissão dos envolvidos, privar alguém de seu direito de liberdade e privacidade ou ocultar conteúdo protegido por força de lei. Guilherme Nucci pondera que:

Para identificação do crime permanente, oferece a doutrina duas regras: a) o bem jurídico afetado é imaterial (ex. saúde pública, liberdade individual etc.); b) normalmente é realizado em duas fases, a primeira, comissiva, e a segunda, omissiva (sequestra-se a pessoa através de uma ação, mantendo-a no cativeiro por omissão). Essas regras não são absolutas, comportando exceções. (NUCCI, 2014, p. 117).

Para o autor supramencionado, crimes permanentes são “aqueles que se consumam com uma única conduta, embora a situação antijurídica gerada se prolongue no tempo até quando queira o agente” (NUCCI, 2014, p. 117). Para Damásio Jesus (2009, p. 189-190), os crimes permanentes “são os que causam uma situação danosa ou perigosa que se prolonga no tempo. O momento consumativo se protraí no tempo, como diz a doutrina”. Já para Cézar Bitencourt (2010, p. 253-254), o “crime permanente é aquele crime cuja consumação se alonga no tempo, dependente da atividade do agente, que poderá cessar quando este quiser (cárcere privado e sequestro)”. Nesta acepção, induz-se a possibilidade de incidência do cibercrime como crime permanente, principalmente em relação aos crimes puros. Vejamos que o bem jurídico, na maioria das vezes, será algum bem imaterial da pessoa, ferirá sua liberdade e majoritariamente sua privacidade, e há também as duas fases, pois o crime se consolida através da ação do cibercriminoso – por exemplo, quando o sujeito ativo do delito virtual divulga ou posta e mantém o conteúdo ilícito – e, em momento posterior, há a atuação permanente e ilícita pelo fulcro virtual até eventual descobrimento tardio da invasão ou extração de benefícios, como o vazamento de conteúdo privado. A base conceitual do crime permanente é a execução do fato típico e não, simplesmente, sua consumação, pois nos crimes instantâneos de efeitos permanentes – como ensina a doutrina – a consumação também se prolonga no tempo. Mas o cibercrime não se confunde com esse último. Afinal, os crimes permanentes são aqueles que, quando consumados, sua execução é realizada permanentemente pela vontade do agente ativo, no caso o hacker ou uma empresa que invade privacidades ilicitamente, como se fosse um ciclo de novas condutas com novos resultados, chegando a novas consumações, de forma contínua. Esta distinção é importante pois haveria discussões acerca da aplicação da súmula 711 do Supremo Tribunal Federal, de aplicação da lei penal mais grave sobre o crime permanente.

Com a aprovação do Marco Civil, a necessidade de ordem judicial foi incluída no ordenamento. O MCI trouxe uma regra específica acerca da necessidade de ordem judicial para

o Estado obter quaisquer tipos de informações privadas e para que o usuário possa ter conteúdo ofensivo retirado:

Art. 7º. O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

[...] II – inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei;

III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. (BRASIL, 2014).

Mas qual a relevância jurídica da incidência de cibercrime como crime permanente? A Busca e Apreensão sem este mandado judicial é possível em flagrante permanente pela preocupação jurídica de cessá-lo imediatamente, engendrando um acometimento mais célere. Nesse caso, não se pode falar em ilicitude das provas obtidas porque o momento consumativo do delito está sempre em execução. O flagrante digital realizar-se-ia quando se descobrisse, por investigação, a localização do suspeito pela identificação da localidade de perpetração do crime, bastando a evidência de que o conteúdo ou a ação delituosa ainda esteja disponível, acessível e em continuidade, de alguma forma, na internet. Assim, asseguraria suas vítimas em detrimento de certas garantias jurídicas do acusado. Tratando-se da mesma lógica dos cibercrimes, o momento consumativo da ilicitude de *hacking* ou divulgação de conteúdo indevido também está em contínua execução (ALVES, 2019b).

Sobre este assunto, em 2015, a decisão do STF no Recurso Extraordinário 603.616 discutiu se e quando policiais podem adentrar domicílios sem mandado judicial com o fito de buscar e apreender droga. Resumindo, o STF estabeleceu que o ingresso forçado em domicílios sem mandado judicial é apenas legítimo quando amparar-se em razões devidamente justificadas pelas circunstâncias indicadoras que no interior da residência esteja a ocorrer situação de flagrante delito. A ilicitude do ingresso forçado na esfera domiciliar tem sido afastada pelo fato de que o tráfico de drogas (ou a posse desautorizada de arma) configuram crime permanente. A princípio, estas razões devidamente justificadas têm de ser legitimamente constatadas. Por exemplo, por não enxergar esses requisitos no HC 138.565 em 2017, a 2ª Turma do Supremo Tribunal Federal concedeu *Habeas Corpus* para trancar a ação penal contra um homem que teve sua residência vasculhada por policiais civis sem ordem da Justiça, encontrando drogas na residência. Ou seja, é uma incidência de flagrante a ser aplicada com a devida diligência.

Afinal, a expressão ambígua que autoriza a realização do ato, as “fundadas razões”, oferece à autoridade judicial certa discricionariedade e subjetividade, podendo ser pretexto de abusos. Entende-se, contudo, que para o seu deferimento, deverão estar presentes a urgência, necessidade e “fortes indícios da existência de elementos de convicção” devidamente

interligado ao processo, não sendo suficiente a simples suspeita como bem aduz Pitombo (2005, p. 128). Jéssica Picolo (2015) elenca outras características juridicamente relevantes do meio cibernético: a transnacionalidade, a deslocalização e a repetição automática. Logo, todo ato criminoso pela internet é permanente, pois uma vez que instalado um programa malicioso ou alterados os dados ou compartilhado conteúdo ilícito e mantendo-o na rede, a cada novo acesso ou compartilhamento a ação criminosa é reiterada.

A Busca e Apreensão é medida institucionalizada que naturalmente viola certos direitos conforme limitações constitucionais e de legislações infraconstitucionais. Por atingir a liberdade individual do investigado, o emprego há de ser com especial cautela, devendo a autoridade violar os direitos do indivíduo o mínimo possível, no momento do cumprimento da diligência, para alcançar os devidos fins na persecução penal. Cleunice Pitombo (2005, p. 91) explicita que “o direito fundamental apenas poderá sofrer diminuição dentro da estrita legalidade”, com legítimos fins e de justificativa socialmente relevante. Para que não desapareçam as provas do crime, a autoridade policial deve apreender todos os itens que tiverem correlação com o delito (art. 6º, II, do CPP). Já o art. 240 do CPP relaciona ainda pessoas e objetos sujeitos à Busca e Apreensão tanto pela autoridade policial como pelo juiz, quando fundadas razões a autorizarem. Apesar da Busca e a Apreensão estarem incertas no capítulo das provas, a doutrina as considera mais como medida acautelatória, liminar, destinada a evitar o perecimento das coisas e das pessoas.

Destarte, cada órgão público deveria fornecer meios os quais o cidadão possa conferir tanto os acessos aos seus dados pessoais, como a motivação do ato administrativo materializado pelo agente público que os acessou, efetivando o princípio da publicidade como preceito geral e do sigilo como exceção, conforme o inciso I do artigo 3º da Lei de Acesso à Informação (Lei n. 12.527 de 2011). Portanto, caso o cidadão discorde com a motivação do acesso (no hipotético caso da Busca e Apreensão por conta de um cibercrime) e perceba distorções quanto aos seus fins, poderá contestá-lo através de um processo administrativo ou ação judicial, como a Ação de Indenização contra a Administração Pública *v.g.* Em caso da comprovação dos fatos ilícitos, deve o suspeito ser autuado; no caso de inocência, deve o Estado prestar contas a este cidadão, apresentando documentos ao mesmo de qual foram as razões e como fora extraído e analisado seus dados. No termo mais comum, *accountability* é primordial para a existência de qualquer regime democrático transparente. Em síntese, Johnson e Wayland (2010, p. 19-33) doutrinam que esta transparência e visibilidade das tecnologias não possuem, ao contrário da transparência democrática, uma conotação positiva porque a transparência sugere a operação da democracia, dos poderosos sendo responsabilizados. Essa *accountability* é de responsabilidade do Estado e

das empresas com seus usuários-consumidores. Atualmente, os provedores ferem este direito do usuário ao utilizar seus dados – como localização e padrão de imagens – sem prévia autorização, como as reportagens de BBC News (2017), Nichols (2018) e Hill e Mattu (2018) exemplificam; já o Estado, ao investigar estes delitos e não oferecer mecanismos para eludir excessos desse próprio Estado. Como veremos no próximo subcapítulo, nos Estados Unidos, há interceptações e violações de privacidade sem nunca o cidadão – de qualquer país – ter conhecimento.

A alteração institucional do MCI aumentou o tempo de resposta do Estado, não trazendo efetivamente maior segurança ao indivíduo, pois um requerimento de busca leva em média 30 dias para ser apreciado pelo juiz competente, enquanto minutos é o suficiente para o cibercriminoso, sabendo do requerimento, apagar seus rastros. Não olvidando que se o Delegado de Polícia estiver imbuído de más intenções, certamente induzirá a erro o Magistrado; por outro lado, também, o Juiz de Direito é passível de cometer abusos. Desta forma, a alteração constitucional aumentou a burocracia e postergou a prestação da tutela jurisdicional. *Exempli gratia* a Lei Carolina Dieckmann não diminuiu invasões a aparelhos de terceiros e a obtenção e divulgação de fotos com nudez alheia; inobstante, sem os devidos meios de efetivação, chegou a atrapalhar (BERETTA, 2014).

Nos Estados Unidos, as agências fiscalizadoras podem renunciar à permissão de um juiz se o agente federal acredita que provas criminais estão prestes a serem destruídas. É justamente o caso do hacker ou empresa cibercriminosa, já que as evidências estão sempre na iminência de serem destruídas pelos mesmos.

Toda vez que o Estado deixa de dar uma resposta célere, fere o direito fundamental dos indivíduos porque diminui o acesso à segurança do usuário e mal administra recursos pela ineficácia investigativa. As instituições policiais são uma das mais vigiadas por organismos do Estado e da sociedade civil, sujeita a controle externo do Poder Judiciário, Ministério Público, Ouvidorias e órgãos fiscalizadores não-oficiais tais como ONGs e imprensa. Em termos práticos, a assertiva democrática diz que “cada indivíduo possui direito igual à mais ampla liberdade possível, compatível com a igual liberdade dos outros”. Com efeito, o direito à privacidade configura, além de um direito fundamental, um direito de personalidade, essencial e inerente à pessoa. Isso significa que a tutela do direito à privacidade visa proteger o indivíduo (ALVES, 2019a, p. 127-138). A falta de regulamentação e tecnologia adequada para combater os casos de violação deste direito dificultam a sua prevenção e repressão, ocasionados, na dicção de Leonardi (2005, p. 42): “pelas mesmas características e peculiaridades que tornam a

internet tão atraente, a tremenda facilidade de disseminação, de busca e de reprodução de informações em tempo real, sem limitações geográficas aparente”.

Como bem já citamos, em 2003, houve a propositura de um método de verificação para verificar qual direito tem peso maior em cada caso. Em síntese, vimos que há uma propensão lógica à consideração do princípio da liberdade de informação em preferência ao direito à privacidade do indivíduo suspeito de fraude. Essa inclinação ocorre porque as vantagens da supressão do direito à privacidade são maiores do que se o contrário acontecesse, como prega o princípio da ponderação de Alexy (2009, p. 91). De qualquer maneira, não deve haver outra opção a não ser a restrição para evitar o dano maior de lesão a outros direitos fundamentais alheios, mediante até do art. 20 do CC, se buscando a solução menos excessiva ou drástica (ALVES, 2019a, p. 127-138).

O artigo 2º do MCI define que o uso da internet no Brasil tem como princípio básico o respeito à liberdade de expressão, todavia, não significa que uma lei infraconstitucional possa modificar o equilíbrio dado pela Constituição. Para o Direito, seria utópico solucionar problemas da internet sem atingir a liberdade e privacidade individual. Por isso, a desnecessidade de mandado judicial nos cibercrimes tem o potencial de ser uma solução.

Até recentemente, somente o autor da presente dissertação havia desenvolvido a tese de interpretação de algum cibercrime como crime permanente (ALVES, 2019a; 2019b). Mas em recente decisão do STF, o Tribunal, por unanimidade, manteve a prisão em flagrante delito, por crime inafiançável, do deputado federal Daniel Silveira e o bloqueio da disponibilização de um vídeo postado pelo deputado no canal YouTube. No que tange esta interpretação, foi esta a decisão do relator Min. Alexandre de Moraes:

As condutas criminosas do parlamentar configuram flagrante delito, pois na verifica-se, de maneira clara e evidente, a perpetuação dos delitos acima mencionados, uma vez que o referido vídeo permanece disponível e acessível a todos os usuários da rede mundial de computadores, sendo que até o momento, apenas em um canal que fora disponibilizado, o vídeo já conta com mais de 55 mil acessos. Relembre-se que, considera-se em flagrante delito aquele que está cometendo a ação penal, ou ainda acabou de cometê-la. Na presente hipótese, verifica-se que o parlamentar DANIEL SILVEIRA, ao postar e permitir a divulgação do referido vídeo, que repiso, permanece disponível nas redes sociais, encontra-se em infração permanente e consequentemente em flagrante delito, o que permite a consumação de sua prisão em flagrante. (BRASIL, 2021).

Evidente que esta decisão não significou que todos cibercrimes, nem crimes cometidos através de YouTube e tampouco vídeos postados criticando o STF serão incluídos no rol de crimes permanentes e cidadãos poderão ser presos em flagrante delito. Foi um caso específico, emblemático e com outra série de nuances, como a questão da imunidade parlamentar do deputado. Porém, inicia-se agora em jurisprudência e doutrinas a discussão sobre esta

possibilidade, que sempre deve ser aplicada considerando caso a caso, especialmente quando as provas estão prestes a ser deletadas.

### 3.1.4 Propriedade Intelectual na Internet

*O que importa são medidas eficazes que asseguram tais direitos.*

São conhecidas as dificuldades que as propriedades intelectuais e os direitos autorais sofrem na internet. As atuais leis de proteção à propriedade intelectual não auxiliam propriamente o combate de infrações cibernéticas e não há praticamente política pública sobre o assunto, exceto campanhas publicitárias demonstrando alguns malefícios da pirataria da TV a cabo e, mesmo assim, não são eficientes. Uma lei que trate de propriedade intelectual deve ser ajustada para simultaneamente: equilibrar os incentivos à criatividade, viabilizar aos potenciais produtores de mercadorias o que os consumidores desejam e minimizar a dissipação do aluguel de alguma obra. No âmbito digital, em vez de tentar obrigar os leitores a aceitar uma reforma particular da doutrina jurídica, o legislador deveria encontrar uma linha de simpatia em seu público e entender as atuais demandas digitais por ferramentas acessíveis.

Antes mesmo dos meios digitais, a propriedade intelectual foi protegida porque os livreiros lucravam com sua atividade e, então, os autores, sentindo-se mal retribuídos, reconheceram que tinham direitos – das obras – que careciam de melhor proteção. Isto por duas razões que até hoje são as mesmas: proteção dos lucros e notoriedade por elas. Em particular, o Brasil se preocupa mais com questões como direitos morais e criatividade da obra pelo autor, ao contrário do *Copyright* que defende mais o direito de reprodução de cópias (PARANAGUÁ; BRANCO, 2009). Por si só, estes dois pontos são suficientes pois, em relação ao fundamento mais usado, o da Teoria do Bem-Estar Social (mais utilitária, com princípios de não-rivalidade e não-escassez), há uma necessidade de recuperação do investimento e de comprovação da personalidade.

Atualmente, empresas, a fim de resguardar seus direitos, identificam o adquirente do produto através do IP (impedindo acessos simultâneos), do login com o uso de CPF vinculado ao produto ou de softwares específicos de acesso ao conteúdo. Dessa forma, trabalha-se com mecanismos de prevenção geral, desencorajando a primeira divulgação indevida e reduzindo consideravelmente a propagação ilícita do conteúdo. Nota-se que o desencorajamento da cultura de desvalorização do trabalho intelectual alheio se dá somente com repressão às

violações de direitos autorais. Então, os titulares de direitos autorais no digital brasileiro devem fazer valer suas prerrogativas legais de proteção a sua obra no INPI, a fim de garantir a remuneração por seu patrimônio intelectual. Afinal, se a produção de informações é cara e difícil, enquanto a cópia é barata e fácil, por que uma empresa, por exemplo, de programas de computador, fará investimentos para produzir novos softwares? Porque, mesmo assim, compensa financeiramente através de suas novas ideias. Em outro exemplo, alguns artistas utilizam a fácil difusão da rede, devido ao acesso barato ou grátis ao material, e o público é atraído para apresentações ao vivo que, finalmente, são as que lhes proporcionam lucros substanciais.

Uma proteção excessiva das obras na rede parece dificultar sua utilização criativa e uma proteção muito fraca já desencorajaria a distribuição de obras de autores que desejam explorá-las economicamente. A complexidade da vida contemporânea tornou a análise e a defesa dos direitos autorais muito mais difíceis. A cultura digital permite que diariamente sejam realizadas milhares de cópias de músicas, filmes, fotos e livros mediante o download das obras na internet contrariamente à literalidade da lei. Afim de tentar proteger os direitos autorais, são criados mecanismos de gerenciamento de controle de acesso às obras, mas tais mecanismos são frequentemente contornados. É cada vez mais comum assistirmos à contestação judicial do uso de obra de terceiros. Vê-se, nesse passo, que a grande questão é a busca pelo equilíbrio entre a defesa dos titulares dos direitos e o acesso da sociedade ao conhecimento ou entretenimento.

O Brasil precisa criar novos modelos de exploração de direitos autorais que efetivamente remunerem o autor a partir do pagamento de valores acessíveis aos consumidores. O consumidor agora acha caro pagar por um CD com poucas músicas ou ir ao cinema para assistir um só filme, mas acha viável pagar uma taxa para escutar ou ver qualquer (ou um bom tanto de) música ou filme – ou seja, todos CDs ou séries e filmes possíveis – que desejar (como com o Spotify ou Netflix). Trata-se de um ajuste de custos-benefícios que mudam durante o tempo e que empresas, artistas e autores precisam se atualizar ou serão perpassadas por conta de ideologias de mercado ultrapassadas. É necessária também uma lei que esteja em conformidade com a vida contemporânea e com as novas tecnologias já que a sociedade não está à margem da lei e sim vivendo no melancólico drama de uma lei à margem da sociedade. O regime penal proposto no Brasil será um dos mais severos do mundo quanto à proteção da propriedade intelectual, gerando consequências políticas e econômicas, além de ser um fator que prejudica a inovação e o acesso legítimo à informação (PARANAGUÁ; BRANCO, 2009).

Nos EUA, para combater a pirataria há algumas normas: Lei de Auxílio de Comunicações para Aplicação do Direito (CALEA), que reforça com que os provedores de

internet e telefonia tenham uma política de grampo sem autorização judicial sempre que for necessário; Lei de Vigilância de Inteligência Estrangeira (FISA), com grampo de grandes potências sem autorização e que o tribunal aceita as solicitações dos congressistas; o Patriot Act, que têm três polêmicos dispositivos: o primeiro é a Lei do Lobo Solitário, em que qualquer pessoa sob vigilância dos EUA tem todos seus dados digitais vigiados (mesmo sem ligação a outros governos), depois temos a Lei da Escuta sem Destino, que trata do controle contínuo e sem consulta a juiz de qualquer pessoa que seja um risco ou que já foi vigiado (ainda que se troque de meio de comunicação), e por fim a Lei de Recolha de Objetos Relevantes, tratando-se do direito dos EUA de recolher qualquer objeto tangível (como documentos pessoais e gravações) de qualquer pessoa que mostre no ambiente digital ser um risco para o Estado, novamente sem delimitação de juiz do que possa ser recolhido; a CIPA (Lei de Proteção à Criança da Internet), ato específico sobre a privacidade de dados online de crianças (menores de 13 anos e 364 dias) que obriga todos os sites pornográficos a usarem a verificação da idade, proíbe a pornografia pública, exige que as escolas monitorem o uso da internet por menores de idade e que conteúdos com material obsceno e pornográfico devam ser filtrados (menos restritivos para adultos); Digital Millennium Copyright Act (DMCA), onde há a criminalização de difusão de tecnologias que contornam direitos autorais; Online Copyright Infringement Liability Limitation Act (dentro da DMCA), que trata da limitação da responsabilidade do provedor; Lei Antipirataria das Coleções de Informações (CIAA), que torna ilegal o uso do conteúdo informativo dos bancos de dados e, assim, protegeria fatos não originais que não são protegidos pela lei de direitos autorais; e a Uniform Computer Information Transactions Act (UCC), no seu artigo 2B da disposição sobre licenças de mercado de massa há a imposição de disposições contratuais referentes às informações, mesmo que concedam aos proprietários do produto informações muito mais amplas do que a lei de direitos autorais.

E há outras três propostas no Congresso do Senado Americano desde 2010 que poderiam trazer grandes mudanças: SOPA e PIPA, que garantem que o Departamento de Justiça e os Departamentos responsáveis pelos Direitos Autorais consigam ir à justiça para que violações sejam tiradas do ar ao bloquear conteúdo do exterior, suspender o pagamento direitos ou verbas, suspender totalmente a publicidade e responsabilizar os provedores; e SISPA, que busca combater cibercrimes incluindo atos cometidos no exterior (rebateria o direito ao anonimato e a questão da competência jurisdicional) ao criar Agência de Vigilância Mundial e uma Plataforma de Ciberinteligência com punições bem definidas, inclusive a empresas e governos (divulgando dados sigilosos).

Ainda sobre a Digital Millenium Copyright Act, a característica mais problemática é o dispositivo que impede o acesso às informações de qualquer pessoa do mundo – como o FBI fez ao impedir que qualquer pessoa no mundo pudesse acessar o Kickass.to ou o ThePirateBay.org, mesmo que todos nós não estivéssemos sob sua jurisdição – independentemente de o reprodutor ter ou não direito legal de controlá-las. A lei americana contorna esses problemas jurisdicionais, mesmo quando a pessoa tem o privilégio de usar as informações. Tudo isto justifica interceptações e violações de privacidade sem nunca o cidadão de qualquer país ter o conhecimento. Como também faz a Regra 41 (UNITED STATES OF AMERICA, 2014) dos Procedimentos Especiais, que concede poderes ao FBI para interceptar qualquer computador suspeito sem reportar-se ao judiciário, isto é, deram-se permissão para invadir qualquer computador do mundo.

No Brasil, o Direito Autoral (DA) serve primeiramente para estimular a criação intelectual com a remuneração fruto do exercício de exclusividade. Com o avanço tecnológico, transformaram-se as formas de autorização, os incentivos para a criação intelectual e até a exclusividade. A outorga do art. 5º, XXVII, da Constituição Federal dá proteção constitucional ao direito autoral com três elementos: categoria da obra, afirmação da exclusividade e sua transmissibilidade. Na construção doutrinária, a associação do DA com Direito de Propriedade (DP) é controversa. De um lado, o DA é um direito de personalidade; do outro, associa-se com o DP, atendendo mais às características morais ou aos elementos de exploração econômica. Sendo o único consenso a existência desta dualidade de caráter patrimonial (de exploração dos direitos patrimoniais, insuficiente na exclusividade temporária) e pessoal (de natureza moral da criação intelectual). Este último limita-se pela função social da obra, que deve equilibrar a garantia dos direitos do autor com possibilidades de utilização da obra por terceiros (SOUZA, 2014).

Os principais dilemas do DA são sobre a extensão da exclusividade e a dinâmica autorização prévia para uso de terceiros. Desde a primeira legislação inglesa de DA, protegeu-se o autor e seu estímulo. Há uma necessária compatibilidade do DA com os progressos tecnológicos e o perigo das limitações freia o desenvolvimento da tecnologia que protege o DA como os *rights managements systems* (DRMs). Com a tecnologia, temos o caso dos autores que renunciam alguns benefícios e amplificam a liberdade do uso alheio, como nas obras colaborativas (pela inclusão de terceiros). O licenciamento, pela autorização, também se modificou, por exemplo com a GPL e a *Creative Commons* (SOUZA, 2014). Um exemplo das supracitadas obras colaborativas é o Wikipédia, que através do *groupware* que utiliza de licença GNU de Documentação Livre torna-se um exemplo de que a liberdade pode gerar benefícios.

Por não haver autorização de ninguém para a modificação de conteúdo, em caso de alterações vândalas por alguém que sem conhecimento ou por motivo alheio ao conhecimento modifica o assunto, teoricamente outra pessoa com o devido conhecimento poderia alterá-la (SOUZA, 2014). Já o maior incentivo de pesquisa científica no Direito, e em outras áreas, na maioria das vezes, não é a exclusividade – aliás o compartilhamento é até estimulado – e sim o reconhecimento. Já sobre o software livre (SL), são quatro suas liberdades: de executar o programa independente da finalidade, de estudo para adequá-lo às necessidades, de redistribuição de cópias e de modificação deste programa. Ou seja, o foco do SL “está nas liberdades concedidas e não na gratuidade” (confusão do termo *free*, significando “gratuito” e também “livre”), por tutela da Licença Pública Geral e, no direito brasileiro, pelo art. 104 do Código Civil. Já a *Creative Commons* é uma ONG que, também por tutela do art. 104 do CC, disponibiliza em seu website três obras modelos de licenças jurídicas para suas veiculações: para leigos, para advogados e código. Por fim, há uma função promocional do DA pela sua essência (da exclusividade como incentivo principal) e pela autorização (da efetivação da exclusividade) (SOUZA, 2014). Felizmente, o progresso tecnológico se revoluciona com a promoção das obras colaborativas, devendo atentarmo-nos a elas futuramente.

Há também limitações aos DA nos casos em que, sem anuência do autor, a obra pode ser utilizada por terceiros, em que o civilista (brasileiro) é mais apegado a noções deontológicas kelsen-neokatianas e o *common law* com influência do pragmatismo autoral de *copyright* mais preocupado com a exploração econômica. Ambos têm diferença no foco temporal: no civilista, o DA existe por realização prévia com impressão da personalidade do autor, equiparando a um direito real de exploração inalienável, com nascimento de trabalho criativo e com limitações por exceções; no *common law*, considerados utilitaristas, todo direito – inclusive o DA – só se justifica pela capacidade de contribuir para o bem-estar comum com aberturas ao autor do trabalho como exceções. O *Copyright Act* dos EUA se refere ao *fair use*, “porto seguro” onde não se aplica a exclusividade como uma limitação, sendo uma proposição funcional estatal válida. Assim, o *copyright* é uma exceção na regra geral do *free speech* (VASCONCELOS, 2014).

O Brasil, de tradição civilista, tem uma relação horizontal para os direitos de mesmo nível, onde essa utilidade esperada não incide. Hodiernamente, não se pode falar em sistemas autorais exclusivamente vinculados a uma tradução somente. No caso brasileiro, as cláusulas gerais deixam para a jurisprudência a definição do conteúdo normativo como a boa-fé ou a onerosidade, a súmula vinculante também tem caráter do *common law* e a própria CF com seu art. 5º, inciso XXIII, estabelece a função social da propriedade. Todavia, pela influência do *doit*

*d'auteur*, a Lei de Direitos Autorais (LDA) brasileira não relaciona a exclusividade a qualquer objeto específico. Tínhamos também o Projeto de Lei n. 3133 de 2012 (apensado ao PL 6117/2009, que foi arquivado) e seus discursos de busca de equilíbrio entre os direitos privados do autor e os direitos difusos de acesso à cultura e à informação, estabelecendo que o bem jurídico tutelado pelo DA não é o trabalho nem a obra em si e sim sua utilidade econômica futura (VASCONCELOS, 2014). Comparando, há lados positivos e negativos em ambas correntes e o legislador deve observar o lado prático das mudanças.

O plágio, especialmente na internet, está *pari passu* com o caráter da originalidade, restando ato ilegal e imoral, com definição na LDA. Há casos brasileiros de plágio de emissoras de TV e alguns tipos de violações por plágio, como a violação à boa-fé. Ou seja, o plágio não se limita aos DAs. Historicamente, Shakespeare, Bach e Mozart tiveram como base de seus trabalhos histórias preexistentes, ou seja, houve acréscimo de algo novo – originalidade – à realidade com contribuição objetiva como aporte intelectual. São as seguintes espécies de plágios com precedentes judiciais: incidental, material, virtual ou ideológico, indireto, mosaico, autoplágio, o quase plágio e o plágio às avessas (GALVÃO, 2014). Para o reconhecimento do plágio, há alguns parâmetros, como os testes de Hermano Durval das semelhanças, da prova circunstancial, das abstrações e o da plateia. Na aplicação de filtros, cita-se três passos deste procedimento: comprovar o acesso, traçar as semelhanças descartando as não elementares e analisar a originalidade. Citemos casos práticos. No caso Apple vs. BRAUN, houve semelhança no design de um rádio e o iPod, com motivo de “inspiração” pelo diretor de design da Apple, Jonathan Ive, que se eximiu. Temos também na jurisprudência americana o Episódio Imperador da Selva vs. Rei Leão em que claramente havia diversas similitudes, mesmo que não houvesse uma ação judicial. Ao aplicar os testes de Hermano Durval, “Rei Leão” é plágio de “Kimba”.

Por fim, há de falarmos sobre a responsabilização dos provedores pelo conteúdo digital. Já tratamos no subcapítulo 2.4.3 das responsabilidades específicas de cada tipo de provedor de serviço da internet (*backbone*, acesso, hospedagem, conteúdo, informação, correio eletrônico, comércio eletrônico e de pesquisa). Uma corrente defende o *Notice-and-takedown*, oriundo da sistemática legal norte-americana e adotado hoje pelo Brasil, em que o provedor, assim que acionado pelo violado ou terceiro interessado, deve retirar imediatamente o conteúdo; a outra corrente é adepta ao princípio do contraditório, em que o provedor, assim que acionado pelo violado, comunica o responsável pelo conteúdo, buscando uma espécie de acordo extrajudicial. E até hoje não há consenso de qual melhor sistema e isto influencia em como será o combate ao plágio nestes meios. Vem prevalecendo a tese da não responsabilidade objetiva pelo provedor, porém deve ele retirar o conteúdo moralmente ofensivo com o deságio de identificar

o plágio. Neste sentido, no Brasil, o STF se posiciona no sentido que o provedor retire ativamente o conteúdo imediatamente pela notificação judicial. De qualquer maneira, temos hoje um alargamento do conceito de plágio e seu aumento repercute no processo criativo, prejudicando artistas e doutrinadores e, por isso, cada país deve impedir o plágio pela internet por métodos mais ativos que a resolução extrajudicial (GALVÃO, 2014). A atual redação do art. 20 do Marco Civil da Internet limita demasiadamente a maior virtude do notice-and-takedown, que permite aos provedores de serviços tomar conhecimento da existência de material ilegal em seus servidores e removê-lo sem a necessidade de medida judicial específica com o mesmo propósito. Bem verdade que o MCI não proíbe esta ação pelos provedores, mas por que a fariam se não são obrigados, se estas ações custam verbas, se são praticamente não punidas pelo mercado pela falta de real concorrência e, principalmente, se errarem em um julgamento interno podem ser processados pelos prejudicados? A judicialização dessas questões, que já se encontravam resolvidas através de outros instrumentos mais ágeis e não jurídicos, atrapalha a tutela dos direitos de usuários. Esta crítica ao notice-and-takedown não só vale para os casos de defesa de PI, mas também para aqueles de infração de direitos fundamentais e de personalidade.

Todavia, este modo também evita uma obrigação de monitoramento injusta e de investir altamente, desencoraja o controle excessivo da rede por poucas empresas e estados, evita uma grande demora na remoção de conteúdos negativos, garante a manutenção da condição técnica de mero condutor neutro dos provedores e encoraja o desenvolvimento econômico da internet (RIORDAN, 2016, p. 7). Ou seja, para beneficiar-se desse *safe harbour*, os provedores não teriam a obrigação de filtrar sua rede em busca de atividades maliciosas. No âmbito de grandes empresas, este filtro poderia ser realizado, mas geraria várias limitações e censuras aos seus usuários. Uma das piores consequências dessa teórica obrigação seria o grande desencorajamento para os pequenos provedores, pois tratar-se-ia de mais um custo, desestimulando novos investimentos neste mercado, aumentando mais ainda o monopólio das poucas companhias que detém a grande parte do mercado. Além dos sistemas de Notice-and-takedown e Notice-and-stay-down, há outros sistemas alternativos como o chileno *notice-and-judicial-takedown*, o canadense *notice-and-notice* e o francês *notice-and-disconnection*, com suas vantagens e desvantagens. Um problema interessante destes métodos é a suposta brecha na lei de direitos autorais que beneficia – criando uma concorrência desleal – alguns provedores, como o YouTube, em detrimento de outros, como o Spotify, o Deezer e o Apple Music, já que estes são forçados a competir com plataformas musicais como o primeiro. O Spotify paga cerca de US\$ 20 por ano por usuário às gravadoras, enquanto o YouTube paga menos de US\$ 1,

sendo que possui 46% do mercado de *streaming on-demand* (IFPI, 2018, p. 26). *Streaming* é a tecnologia de transmissão de multimídia pela internet sem a necessidade de baixar o conteúdo, com consumo contínuo sem armazenamento. É o método de entrega do conteúdo e não ao conteúdo em si.

Outro problema na rede é caso o do BitTorrent. Estima-se que em 2004 e 2005 só esta plataforma foi responsável por 35% de todo tráfego de dados da internet. Atualmente, durante a pandemia da COVID-19 (*Coronavirus disease*) desde o ano de 2020, os números de download por torrents se multiplicaram. O BitTorrent e o  $\mu$ Torrent detém hoje 75% deste mercado (VAN DER SAR, 2020) e foram comprados pela empresa de criptomoedas Tron por US\$ 140 milhões de dólares. A BitTorrent alega ter hoje 40% do tráfego de dados da internet (VAN DER SAR, 2018) e outras fontes alegam que ela domina 22% do tráfego global de *upstream*, onde 15% do total dos downloads na internet são *streaming* de vídeo da Netflix, mas a BitTorrent lidera em uploads (SANDVINE, 2018). Lembrando que foi comprada sabendo-se que a maioria de seu uso é ilegal. Num sistema de servidor central, os usuários dependem do funcionamento deste servidor para enviar ou baixar arquivos, tornando o processo mais lento ainda quando são torrents mais pesados e que são baixados por várias pessoas ao mesmo tempo. Já no BitTorrent ou em qualquer outro sistema de compartilhamento deste tipo, se otimiza o desempenho geral de rede, uma vez que não existe fila de espera e nem sobrecarga por múltiplas utilizações e todos partilham partes do mesmo arquivo entre si, no sistema de pares peer-to-peer (P2P). Pelo contrário, quanto mais utilizadores entram para descarregar um mesmo arquivo, mais largura de banda se torna disponível. Até quem tem apenas parte do arquivo também o compartilha. Inicialmente criada para distribuir arquivos de forma legal, sem violar nenhum *copyright*, trailers de filmes ou qualquer outro material de livre distribuição, o BitTorrent e o  $\mu$ Torrent também são conhecidos por terem na rede usuários partilhando músicas, filmes e programas ilegalmente, assim como acontece com as outras redes P2P. Apesar de outros sites serem os responsáveis diretos pela disponibilização do conteúdo ilegal para download (como o ThePirateBay, KickAss e Rarbg), eles fornecem o meio, sendo controversa qual seria sua responsabilidade. Um dos casos famosos foi a disponibilização do filme “Matrix Reloaded” (2003) um dia depois do lançamento no cinema, outro foi o vazamento do código fonte do jogo “Half-Life 2” e até houve compartilhamento de parte do código fonte do Windows NT e do Windows 2000. Aliás, governos tentam até hoje derrubar ou, pelo menos, indisponibilizar estas plataformas com conteúdos ilegais em seus países, inclusive o FBI, mas logo após a derrubada do site oficial (como com o próprio ThePirateBay.org ou no caso do KickAss.to), usuários e apoiadores da causa criam outro link de acesso para os usuários, inclusive podendo

encontrá-los em uma pesquisa rápida pelo Google (principalmente porque o servidor não é desativado ou destruído, mas tão somente um dos acessos a ele). Com programas de mascaramento de IP (utilizando um de outro país), é possível que usuários utilizem estes sites mesmo com o acesso estando bloqueado em seus países.

Até o momento, o BitTorrent e o  $\mu$ Torrent são o protocolo P2P mais popular adotado para usos legalizados. Existem duas diferenças principais entre eles e outros compartilhadores comumente conhecidos. Primeiramente, eles não oferecem um sistema de busca interno, o usuário deve procurar os arquivos torrentes que apontam para o arquivo que ele quer baixar por indicação de sites que indexam torrentes. E em segundo lugar, a rede não dá suporte ao usuário para distribuir um arquivo, ele deve rodar um *tracker* – localizador – para tornar o seu torrente disponível por conta própria ou com um *tracker* de terceiros. Essas duas características tornam a rede BitTorrent ou  $\mu$ Torrent e seus usuários alvos improváveis de processos judiciais, pois operariam como uma “especificação tecnológica neutra” (WANG, 2014, p. 166, tradução nossa). Porém, o mesmo não se pode dizer da maioria dos sites compartilhadores, pois rodam *trackers* ou sites indexadores de torrentes para distribuição ilegal de programas comerciais, jogos, filmes completos, músicas e pornografias. Mas enquanto não houver evidências de alguma editoração ou autoria, os tribunais dificilmente concluirão que há conhecimento da sua atividade como ilegal. Afinal, defender o contrário pode colocar em risco a legalidade de outros serviços comumente usados como Amazon MP3, iCloud, Dropbox, Gmail ou OneDrive, que envolvem grandes quantidades de material infrator (além do conteúdo legal) armazenado por usuários em servidores remotos. Assim, os tribunais podem ser relutantes em tratar da legalidade destes serviços amplamente populares habilitados por novas tecnologias, como computação em nuvem e armazenamento (WANG, 2014, p. 177).

A PI e a segurança digital não possuem políticas públicas de fiscalização eficazes. Legislações elementares, mas que asseguram na prática seus patenteadores podem ser o suficiente, mesmo normas principiológicas básicas que, em um sistema *common law* por exemplo, permitem juízes ter base para formar a segurança jurídica daquele país. Políticas públicas surgem de suas positivamente, mas devem ir além. O Brasil tem excelência quanto ao seu ordenamento jurídico, tutelando até mais direitos – muitos deles fundamentais e democráticos – que o próprio EUA e outros países e, pelo Marco Civil, traz princípios bem definidos e importantes para a internet. Todavia, todo este ordenamento benquisto mascara a realidade de um péssimo serviço de patenteação e de um dos piores asseguradores dos direitos – inclusive o intelectual e autoral – dos ciberusuários. Normas jurídicas e políticas públicas não são inversamente proporcionais; ao contrário, deveriam se coincidir.

A pirateação não ocorre por culpa da legislação e sim por conta do desenvolvimento tecnológico de cibercriminosos que acompanham – na verdade, ultrapassam – as medidas de empresas e de todos Estados. Mesmo assim, em exemplos como os jogos eletrônicos, tem-se notado que fãs ainda buscam mais os originais. Deve-se considerar a evolução de diversas plataformas e aplicativos dos mais variados conteúdos, como por exemplo: culturais (*streaming* e audiovisuais); financeiras (bancos digitais e captação de investimentos); educativas (websites informativos); dentre tantos outros que, com custos muito mais acessíveis e ideias inovadoras, facilitam e melhoram diversas atividades. Dentro dos culturais, podemos citar *streamings* musicais como o Spotify, Deezer e Amazon Music, os *streamings* de filmes e séries como a famosa Netflix e a Amazon Prime Video, de vídeos como YouTube Pro, além das plataformas de livros como Kindle, da Amazon, e LEV, da Saraiva. Diante de excessos de proteção, há sentido quando Paranaguá e Branco (2009, p. 89) dizem que “as restrições tecnológicas anticópias acabam por prejudicar os melhores consumidores da indústria cultural, justamente aqueles que pagam corretamente pelos produtos adquiridos”. É necessário utilizar essas inovações digitais em prol de uma proteção intelectual mais eficaz, transparente e ágil em um trabalho conjunto da sociedade, pois a legislação já está bem feita, faltando só a eficácia na fiscalização e ainda maiores criatividade de mercado.

Observando a experiência americana já mencionada, é possível adaptá-la ao Brasil? A maioria diz que são possíveis poucas comparações devido às diferenças político-jurídicas de cada um deles, a clássica argumentação dos cuidados do uso do direito comparado, especialmente na comparação entre legislações de *common law* e de *civil law*. Mas ao contrário destes estimados colegas, cremos ser possível tal comparação neste caso, pois política pública quanto à fiscalização é escolha do executivo ou do legislativo quando abstrai uma suposta vontade popular. Poderia o Brasil fiscalizar (mais) seus internautas e a realidade social, jurídica, econômica e política diferente entre os países não influenciaria esta escolha. Mesmo quanto à proteção de PI, deve o Brasil, através de seus órgãos, fiscalizar e assegurar melhor suas patentes e propriedades intelectuais e autorais. Em âmbito internacional, nosso país tem total autonomia de se aderir ou não às convenções internacionais e de se defender quanto aos malefícios de ordenamentos internos e internacionais. Já se há concordância ou não com os métodos americanos, cabe melhor análise.

Como vimos, os EUA fiscalizam o máximo possível todos os internautas globais – inclui-se aqui empresas e outros Estados – através de mecanismos como PRISM, XKeyscore ou ECHELON (como demonstrou o Snowden) e, quanto à proteção de PI, protegem bem suas patentes e propriedades intelectuais, tanto que são os maiores detentores de patentes junto à

China. Por outro lado, não é satisfatório como o Brasil trata atualmente suas patentes, com burocracias e morosidades extremas – em 2013 a espera era de 13 anos com uma taxa absurda de 980 pedidos de patentes por examinador; na Europa, eram 77 (WIPO, 2013); e hoje não é muito diferente – e, tampouco, como perde em âmbito internacional como na disputa DS 199 (WORLD TRADE ORGANIZATION, 2001) em que nosso país aceitou praticamente pedir permissão para os EUA toda vez que for pedir licença compulsória a empresas americanas. Parece-nos que o Brasil poderia sim aprender com a asseguaração de patente dos EUA ao melhorar seus serviços. Na visão liberal, se os EUA têm mais patentes é porque oferecem um melhor sistema; na ótica intervencionista, asseguram devidamente suas patentes com boas políticas públicas e monopólios de ótimos resultados financeiros.

A necessidade de segurança digital e sua conciliação com as PIs não é em detrimento um do outro. Não há sentido no receio de que o Estado poderia abusar da patente ou da propriedade intelectual quando seu monopólio as assegura. Independente da política de segurança digital completamente violadora de direitos de todos países, é possível velar as PIs como demonstram os EUA. Quanto ao Brasil adotar as medidas de segurança da internet dos EUA, poderíamos começar aos poucos já que, com uma Polícia Federal que resolve algumas dezenas dentro de milhares de casos, polícias civis com taxas menores que 5% de resolução de casos e um Judiciário extremamente moroso, difícil é ser pior do que já é, mesmo com suas leis benquistas. Na busca pelo equilíbrio ideal, nenhum país chegou perto de encontrá-lo e com uma razão: ou se fiscaliza seus cidadãos ou não se fiscaliza. Não existe meio-termo porque, infelizmente, quando o país não quer impor mínimas obrigações e fiscalizações, há sempre a ineficácia de asseguarações de direitos. A comunidade jurídica busca palavras como democracia e equilíbrio, enquanto os EUA, por exemplo, se deram conta de algo que no Brasil não descobrimos ainda: a lei não importa tanto, para ela existe a interpretação extensiva e principiológica, o que importa são medidas eficazes que asseguram tais direitos.

Complementarmente, interessantes são os casos de combate à pirataria na Alemanha e França. A legislação alemã dá poder a entes privados, como os estúdios detentores dos direitos autorais de filmes e seus escritórios de advocacia com equipes de TI especializadas, para que monitorem sites de downloads de torrentes em busca de conteúdo que viole seus direitos autorais. Caso identifiquem tal infração, notificam o usuário a pagar certa multa corretiva pelo crime ou ele sofrerá um processo judicial. Já a França possui um órgão que monitora redes peer-to-peer (P2P) e notifica através de e-mail os usuários que transgridam a lei. Caso o usuário persista no crime, um juiz avalia o caso e pode determinar multa e/ou a suspensão do acesso à internet deste usuário. Seus Estados entenderam a necessidade de uma coibição através de

vigilância, inclusive a terceirizando. Até que ponto estes entes privados adentram os dados pessoais dos usuários e como garantem a segurança deles? Aliás, estes entes identificam IPs dentro de cookies de servidores destes websites através de uma espécie de hackeamento. Então por que não solicitar simplesmente a remoção destas páginas ou por que eles mesmos não a derrubam se já a hackearam de alguma forma? Parece ser este modo preferível devido ao maior lucro que podem obter com estas multas. Já o caso da França expressa melhor a questão da tutela estatal. Como conseguem os Estados (e os entes privados terceirizados e aqui jaz uma outra série de problemas) monitorar a rede? Geralmente, os Estados de todo o mundo, especialmente nos EUA, realizam pactos com os provedores de acesso, que muitas vezes são obrigados, para que estes abram suas plataformas a fim de que estes entes estatais e privados terceirizados acessem todo conteúdo de todos usuários do país. Assim como ocorre no Brasil, os Estados obrigam os provedores existentes e fornecem uma espécie de pré-acordo com esta condição antes mesmo de um provedor iniciar suas atividades no país. Tudo isso sem anuência do ciberusuário com a justificativa do bem-estar do mesmo, como ao proteger certo estúdio, este obtém os seus devidos recursos a fim de continuarem suas atividades para o bem coletivo.

De qualquer maneira, o Brasil pode aprender a partir dos EUA e da UE ao deslocar a preocupação com produção de leis à eficácia de melhores métodos de fiscalização e patenteação. Nos EUA, ao descobrirem das polêmicas do Snowden e da NSA, a comoção pública foi mínima porque sentem-se seguros. Na visão de patenteador ou como internauta, ao patentear e demorar 15 anos para obter uma licença e ao ter uma Polícia que demora anos para solucionar um cibercrime que você tenha sido vítima, existe realmente segurança jurídica?

### **3.1.5 Restrição Publicitária e Indisponibilização de Conteúdos**

*A restrição publicitária, quando necessária, é uma questão de justiça.*

Um ponto divergente do meio digital é a restrição estatal de conteúdo considerado inapropriado. Numa perspectiva liberal, se a demanda por material minimamente obsceno, imoral ou ilícito é virtualmente inexistente na superfície da internet, isso impediria, pela lógica de mercado, que todos empresários deixassem de fazer propagandas maliciosas. O que não ocorre. Depender da boa-fé de empresários e submeter consumidores à conteúdos maliciosos, para que estes não se interessassem pelo produto – levando à não reprodução desta propaganda – é desnecessário, quando várias entidades assim podem evitar.

Houve propagandas que, quando liberadas pela CONAR como exemplos de seus vetos, nos certificaram de que o conteúdo realmente deveria ter sido indisponibilizado, pensando na hipossuficiência do consumidor. Na teoria, faz sentido que a empresa não possa se dar ao luxo de se associar a algo que público não gostará, porém, na realidade da falha humana e de atos ilícitos independentes de boa-fé, propagandas danosas não podem se perpetuar. Trata-se de um cálculo de custo benefício que evidencia a insuficiência da suposta liberdade de julgamento do consumidor perante tamanhos malefícios da propaganda danosa.

Qualquer limitação em direitos fundamentais – a liberdade de empresários de fazer propagandas como bem decidirem – significa restrições ao acesso à informação da sociedade como um todo e à saúde da democracia. Pois, de fato, restrições às liberdades individuais devem ser evitadas e quando atingidas, deve haver fundadas razões. O caso em questão não é diferente, a necessidade de um Direito Digital e a restrição supracitada com a avaliação por uma agência reguladora como a CONAR são de mister importância para todos consumidores.

A restrição publicitária, quando necessária, é uma questão de justiça e não de censura. Caso os profissionais publicitários se autorregulassem eficientemente, respeitando a sociedade e seus consumidores em detrimento do lucro, certamente não precisariam defender uma intervenção liberal tão drástica. Inclusive, ser contra a restrição poderia se classificar como anticapitalista, pois atenta contra o sentimento de confiança – em ligar a televisão e ver uma propaganda que respeita os mínimos direitos fundamentais e o bom senso – necessário para a manutenção do capitalismo. Sem esta restrição publicitária, seria necessário este imenso depósito de confiança no comércio, no produtor e no anunciante, porém a desconfiança do brasileiro no livre mercado tem respaldo nas práticas de desrespeito por parte de empresários e publicitários, tanto em nosso país quanto no resto do mundo (MEUCCI, 2015).

São ainda mais raros os liberais que defendem a publicidade infantil, proibida no Brasil. Crianças teriam capacidade para assimilar as informações divulgadas nos meios de comunicação e fazer escolhas devidamente racionais? Para decidir, uma criança ou pré-adolescente precisaria estar em posse plena das faculdades racionais, o que não é possível. Não é necessária a psicanálise de Freud para provar que, nos primeiros anos de vida, os humanos são regidos pelo inconsciente, pelas fantasias infantis, sem qualquer operação racional capaz de analisar informações complexas. Pode-se afirmar que crianças e jovens não apresentam plenas faculdades racionais. Assim, não há sentido propagandas que estimulam seu consumo, pois nessa faixa etária não conseguem escolher, tão bem quanto um adulto médio, o que é melhor para si, gerando uma espécie de lavagem cerebral em pequena escala em pessoas incapazes. Pode-se afirmar que toda comunicação direcionada às crianças tenta persuadir esse público

utilizando-se de um discurso lúdico, pois é um público incapaz de tecer um julgamento plenamente racional. A criança, na maioria das vezes, não sabe se os produtos estão dentro do orçamento da família, se são seguros para sua idade, se o consumo de certos alimentos como salgadinho, bolacha ou refrigerante pode desencadear em problemas como alergia, obesidade, pressão alta ou aumento da ansiedade (MEUCCI, 2015).

Em países como a Suécia, de forte tradição democrática (diferente de liberal), a publicidade voltada para o público infantil já foi abolida há muito tempo por mecanismos de regulação de conteúdo. Aliás, é difícil encontrar país que defenda tal negligência. Outro caso é a classificação indicativa de programas que informa a faixa etária apropriada e em que horário deve ser exibido, visando a proteção da infância e tratando-se de uma importante regulação de conteúdo. A proteção da infância não fere a liberdade de expressão e, neste caso, o conteúdo também precisa ser regulado (EKMAN; BARBOSA, 2015). A liberdade individual autoriza as pessoas a se colocarem em perigo quando conscientes do risco, exceto aqueles que não estão em plena posse da faculdade racional: as crianças e os desvairados. Se uma comunicação publicitária induz a uma compra que coloque as crianças ou a comunidade em risco, ela deve ser proibida para evitar danos. A argumentação do liberal lúcido é muito clara nesse ponto. John Stuart Mill, defensor radical das liberdades individuais de comércio, advertia sobre o problema infantil em seu livro:

Talvez seja desnecessário dizer que esta doutrina se aplica unicamente aos seres humanos que atingiram a maturidade de suas faculdades. Não nos referimos, portanto, às crianças, ou aos adolescentes os quais sua idade seja menor à aquela determinada por lei, exemplo: lei da maioridade. (MILL, 2000, p. 17-18).

A UNESCO (Organização das Nações Unidas para a Educação, a Ciência e a Cultura), que não representa uma organização autoritária, entende que há muitos motivos para a regulação de conteúdo nos meios de comunicação de massa: promover a diversidade cultural; assegurar proteção dos indivíduos contra material que estimule o ódio, à discriminação e ao crime e contra a propaganda enganosa; proteger crianças e adolescentes de conteúdos nocivos ao seu desenvolvimento; proteger a cultura nacional, entre outros. Ao estabelecer que não mais de 25% da grade de programação de uma emissora sejam ocupados com propagandas e anúncios, o Código Brasileiro de Telecomunicações também regula o conteúdo para o bem do cidadão (MEUCCI, 2015).

A submissão de crianças a propagandas danosas a fim de que “aprendam com a experiência de vê-las” mostra-se improdutiva. São imprudentes tais discursos de legitimação da propaganda infantil mediante possíveis benefícios – alguns pautados na propaganda como

meio de aprendizado de escolha, experiência de vida e de avaliação de informações – quando não devidamente avaliados os malefícios do aumento da responsabilidade dos próprios atos das crianças. Outra analogia utilizada é a de que “se as crianças hoje estão com sobrepeso, não é culpa da propaganda do McDonald’s e sim dos pais que permitem”. Vimos que propagandas podem alterar até a fisiologia e as emoções mais íntimas de qualquer ser humano, não restando o que poderiam pais consertarem quando já está impresso na psique da criança certo reforço positivo. A consolidação na prática do desejo despertado injustamente na criança de um produto, a qual ela desconhece grande parte de malefícios e benefícios por falta de experiência, é sim de responsabilidade dos pais. Porém, a responsabilidade de colocar a ideias nocivas no costume das crianças, neste caso, é da propaganda. Mesmo sendo os filhos de inteira responsabilidade dos pais perante a consolidação prática do desejo, os mesmos não podem controlar os ideais nocivos que propagandas normalizam aos seus filhos. Para um mínimo de segurança e de conteúdo aceitável, a restrição se faz necessária, indo além da crítica liberal de superproteção parental a ponto de encapsulá-lo numa espécie de bolha social. A responsabilização dos pais não exclui o das propagandas.

Outro aspecto são conteúdos de propaganda e de mídia em geral os quais atingem de forma direta e minimamente agressiva. Não se é capaz de defender uma ideia ou propagar uma informação sem se desvencilhar de suas próprias crenças ideológicas e de seus valores culturais e políticos. Tampouco é possível haver concordância entre todos, quando uma informação sempre tem o potencial de alcançar alguém que desagrede. A assertiva democrática diz que “cada indivíduo possui direito igual à mais ampla liberdade possível, compatível com a igual liberdade dos outros” e, para esta subjetiva avaliação, o Estado é o melhor julgador. Ou seja, a inviabilização de conteúdo na internet, como propagandas nocivas, na avaliação pelo Estado, deve considerar caso a caso para verificar se houve algum direito atingido além do mero aborrecimento ou da discórdia entre ideias. Na lógica liberal, o consumidor assume o risco ao assistir certo comercial ou comprar certo produto e, mediante a oferta e demanda, basta não voltar a assisti-lo ou o canal e deixar de comprar o produto que automaticamente a propaganda não mais teria maiores razões para existir. Mas como descrevemos, o empresário erra e comete atos ilícito, sendo necessárias restrições a fim de proteger o consumidor-cidadão.

Observando caso a caso do conteúdo a ser indisponibilizado ou não pelo Estado, existe respaldo na Constituição Federal:

Art. 197. São de relevância pública as ações e serviços de saúde, **cabendo ao poder público dispor, nos termos da lei, sobre sua regulamentação, fiscalização e controle, devendo sua execução ser feita diretamente ou através de terceiros e, também, por pessoa física ou jurídica de direito privado.**

[...] 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.

[...] § 2º **É vedada toda e qualquer censura de natureza política, ideológica e artística.**

§ 3º Compete à lei federal:

[...] II – **estabelecer os meios legais que garantam à pessoa e à família a possibilidade de se defenderem de programas ou programações de rádio e televisão que contrariem o disposto no art. 221**, bem como da propaganda de produtos, práticas e serviços que possam ser nocivos à saúde e ao meio ambiente.

Art. 221. A produção e a programação das emissoras de rádio e televisão atenderão aos seguintes princípios:

[...] IV – **respeito aos valores éticos e sociais da pessoa e da família.** (BRASIL, 1988, grifos nossos).

Os anúncios publicitários, que são regidos pelo CDC, devem seguir princípios básicos. No da Identidade, toda publicidade deve ser identificável como tal, não se pode divulgar algo ao consumidor sem que este saiba que está sendo alvo de anúncios comerciais. Na internet, este caso é paradigmático. Vide o emblemático episódio 266 do seriado animado “South Park”, muitos sites utilizam-se de postagens sobre celebridades, curiosidades e outras informações para disfarçar anúncios e propagandas, sempre buscando subjugar o consumidor a condicionamentos (através de reforços positivos) artificiais de comportamento ao estilo de Edward Bernays. Ele foi um pioneiro austro-americano que substituiu a palavra propaganda por relações públicas por causa do contexto nazista que se utilizou dessa ferramenta para uma espécie de “lavragem cerebral” em sua população. No Princípio da Transparência, fornecedores devem expor informações amplas a respeito do produto. Temos hoje em propagandas de remédios, ao seu final, uma tela azul com um grande texto branco impossível de ser lido pelo curto tempo de praticamente 3 segundos e a frase dita “Em caso de sintomas o médico deverá ser consultado”. Esta medida é quase tão inútil quanto o consentimento tácito já citado sobre os dados pessoais do consumidor. No da Veracidade, são proibidas informações – inteira ou parcialmente – falsas ou que simplesmente omitem verdades sobre os produtos que o induziram ao erro, em que empresas utilizam esta margem subjetiva ao clamar seus produtos ou serviços como os melhores do mercado. E finalmente há o Princípio da Correção, que proíbe a publicidade abusiva (NUNES, 2008, p. 842-846). Podendo-se encontrar nestes princípios todos motivos da regulamentação da restrição de conteúdo, neste caso de propaganda, quando atingir negativamente o consumidor.

O Código de Defesa do Consumidor regulamenta a oferta e a publicidade (arts. 30 a 38), especialmente a propaganda enganosa (art. 37, §1º). E na situação de publicidade, a maioria dos websites possui propagandas terceirizadas. Apesar desses terceiros pagarem aos provedores para utilizarem parte de seus websites, a princípio, esses provedores não se responsabilizam

pela falta de prestação de serviço ou defeito de produto deste terceiro (RIO GRANDE DO SUL, 2009a).

Todavia, há exceções de responsabilidade desses provedores: quando recebem comissão dessas transações (geralmente porque a comissão é descontada já na contratação do serviço ou na venda do produto, como no Mercado Livre e na OLX Pay), bem como quando apresentam um sistema de qualificação não tão seguro (art. 14, §1º, CDC) ou ainda fazem parte da cadeia de consumo (art. 7º, parágrafo único, CDC) influenciando na compra. Neste caso, há responsabilidade solidária do dono do site com aqueles fornecedores que não cumprem os contratos naquele espaço (DISTRITO FEDERAL, 2008).

Argumentos que justificam o término das restrições como o de que “na verdade, se o Estado tivesse educado e informado devidamente seus cidadãos a repudiar conteúdos danosos aos mesmos, não se precisaria das restrições”, mesmo que sejam uma verdadeira premissa, não afastam a necessidade desta restrição publicitária. Aceitar que uma criança seja exposta a apelos mercadológicos, contando com a boa vontade de empresários, é a melhor forma de lidar com essa questão? Dizer que a regulação de conteúdo não deva existir é um ato de má-fé ou, no mínimo, uma conduta muito mal informada e utópica (EKMAN; BARBOSA, 2015).

Este cuidado especial com as crianças e adolescentes também existe na proteção de seus dados pessoais. Por exemplo, mesmo que haja um prévio consentimento delas ao apertar em “Concordo” em um Contrato de Adesão digital, poderia a empresa se utilizar de suas informações para a propaganda direcionada ou até para comercializar seus dados? Como consenso na doutrina e na jurisprudência, não podem os provedores fazerem uso das informações de crianças e adolescentes para a propaganda personalizada. Mas na prática, não há acesso possível a dados oficiais certificando que as empresas cumprem esta determinação.

Assim, o Brasil, como qualquer país, deve se assegurar de que utiliza as melhores ferramentas jurídicas de respeito aos princípios básicos constitucionais para limitar liberdades individuais. Todavia, existem casos extremos a serem evitados. É o caso da Coreia do Norte. Lá existe internet, mas com acesso restrito e dependente de autorização do governo. Só para possuir um computador na Coreia do Norte é necessária uma autorização. O Ministério dos Correios e Telecomunicações da Coreia do Norte já bloqueou oficialmente o Facebook, Twitter, YouTube e outros websites na tentativa de controlar ainda mais o acesso às informações que chegam ao país. As recentes restrições são iguais às medidas de censura na China, que possui um grande *firewall* de bloqueio administrado pelo governo. Estima-se que mais de 2 milhões de norte-coreanos utilizem celulares e poucos conseguem acesso à internet, algo limitado aos funcionários e pessoas com permissão do governo (TALMADGE, 2016). Só um pequeno grupo

de privilegiados – estima-se 100 pessoas entre 25 milhões de habitantes – tem acesso real à internet com apenas 1.024 IPs registrados até 2014 (MONTEIRO, 2014). Estrangeiros, entre turistas e jornalistas, também possuem acesso à internet, exclusivo nos hotéis onde são hospedados e em *lanhouses* específicas, com acesso previamente permitido a notebooks e celulares individuais. O contexto democrático atual é incompatível com estas políticas governamentais tão autoritárias. Hoje o acesso à internet deve ser livre e exemplos como estes devem ser evitados.

### 3.2 TÉCNICA ELLULIANA NA INTERNET

*A internet aliena o homem de tantas formas.*

Como vimos, de acordo com Ellul, a técnica caracteriza-se pelo automatismo, autoacréscimo, unicidade, universalismo, autonomia e ambivalência, além de racionalidade, artificialidade, alienadora, misantropa, sem finalidade e com efeitos imprevisíveis.

Quanto ao automatismo, dificilmente um ciberusuário escolhe uma ferramenta de uso na rede que não seja a mais eficaz possível no que faz. Logo, não temos uma verdadeira escolha entre tantas possibilidades. Pode parecer que há liberdade de escolha entre *apps* e websites e mesmo que haja algumas opções, vejamos o quanto suas características são parecidas, suas funcionalidades as automatizações de nossos movimentos para efetuar uma ação. Somos e ficamos condicionados a “(des)curtir”, “amar”, “compartilhar”, “comentar”, “marcar”, “salvar” e rolar o dedo indicador ou o polegar para ver mais e mais de conteúdos que nos desinteressamos menos e menos.

Já o autocrescimento na internet pode ser observado quando ela suscita problemas de natureza técnica que exigem soluções que só um programador pode resolver com mais códigos. Os processos em cadeia excluem cada vez mais o homem de suas necessidades, a mecanização de todo processo chega ao ponto que inteligências artificiais estão conseguindo criar e corrigir códigos sozinhas, vide exemplos como o ChatGPT, ou aprender nossos padrões comportamentais a fim de gerar experiências personalizadas de tal maneira que nenhum outro ser humano poderia fazer igual. Até quanto deverá crescer exponencialmente a internet, os dados e a tecnologia? Não é futurista pensar que, em breve, IAs poderão prever e estimular com precisão hormônios (da felicidade, do prazer, do relaxamento ou da recompensa) através do que nos é mostrado em telas, fazendo nos sentirmos “mais felizes”, o que geralmente significa: mais

entorpecidos da dura realidade. Já não nos é mais estranho o surgimento de posts ou propagandas sobre coisas que só pensamos e nem pesquisamos ainda. O autocrescimento da internet é tal que uma empresa ou empreendedor ou até trabalhador que não está no mundo real-virtual dificilmente sobreviverá, condicionando cada vez mais entes e indivíduos a utilizá-la. A internet torna-se, então, uma necessidade.

Vimos que internet é o conjunto de *hardwares* e *softwares* que interconectam, por meios de comunicação, informações. Usar a internet é utilizar este conjunto, esta tecnologia. É o interagir com a máquina. Veja então que não há uma separação desta internet do uso a que ela é destinada. Nesta unicidade, só é viável utilizá-la da maneira mais eficaz possível.

Algumas pessoas estão fora da rede. Algumas a utilizam moderadamente e alguns somente para trabalho. Mas todos governos a tutelam de uma forma e a maioria das pessoas está submetida à internet e às suas repercussões. Uma destas é a redução das culturas. Cada vez mais, esta globalização tecnológica através da cibercultura padronizada está condicionada aos modismos sociais, como a “lacração”. Nossas reações na rede são praticamente automatizadas. Comentários e posts são previsíveis, levando a massa de ciberconsumidores a serem facilmente manipuláveis. Além disso, o ser humano vai perdendo seu senso crítico e as opiniões se tornam indiferentes. Ninguém liga mais para a opinião do outro na rede. A internet de hoje é uma plataforma de julgamento frio dos atributos alheios. Há resquícios de simpatia e empatia, de boas ações, posts educativos, páginas e perfis que buscam ajudar e educar o próximo, *tweets* elucidativos e uma útil transferência de informações e dados. O resto é julgamento. E mesmo nestes bons casos, qualquer deslize em uma postagem ou margem interpretativa de palavras que derem brecha, é certo que serão apedrejados pela mesma mão que os afaga. O ciberusuário julga veemente e o mais rápido possível pelo medo da exclusão social. E pelo medo de ser o próximo a ser julgado, torna-se dependente de adaptar-se dentro do que é aceitável e não-lacrável na rede. Diria Ellul que a internet é a nova evidência indiscutível, tornando qualquer outro meio de comunicação inútil neste mundo do espetáculo de ícones. Estes são os viralizados, *digital influencers*, políticos, agentes de propaganda e empresas, os digitais formadores de opinião, artistas e (sub)celebridades, que expõem suas opiniões como verdades e, geralmente, divulgam suas ideologias a fim de atacar as demais formas de viver, ser e pensar.

Chegamos ao ponto em que tudo que a internet permite que seja realizado é justificado, não significando ser todas ações lícitas na rede. É muito comum que pessoas, mesmo sem recompensa, defenderem qualquer atributo da internet, como a necessidade de existir cookies para se acessar um website. Parece ser a internet uma entidade autônoma. É certo que humanos tomam decisões que modificam a rede, mas cada vez mais mecanizada, parece a internet ganhar

vida de tal forma que nem os CEOs das grandes companhias da rede, como o do Facebook Mark Zuckerberg, parecia ter o completo domínio sobre o que sua rede social faz.

No cérebro, temos uma parte responsável pelo neurotransmissor dopamina, aquele que gera a sensação de prazer e de bem-estar com a vida. Quem consome muito a rede social passa por três fases: na novidade, atinge picos de prazer de dopamina; na continuidade, o ser humano se adapta à quantidade de dopamina (estágio de homeostase, equilíbrio de saúde e tolerância), inclusive isto tem muito a ver com o vício porque vai se ficando mais tolerante (menos sensível a estímulos), mas ainda remove sensações negativas; no final, está o homem preso e não há nem diversão em jogos e em redes sociais e mesmo assim você não consegue parar (vício biológico). Afinal, pegar o celular por impulso (dopamina fácil pelo “circuito do triunfo”) para ler todas mensagens e e-mails serve a uma espécie de recompensa. Isso faz com que dificuldades da vida real são extremamente indesejáveis, pois são muito mais difíceis que conquistas no mundo virtual. Além do vício biológico, a internet também aliena o ser humano a escolher realmente uma só ação, a mais eficaz. A ambivalência da internet é esta inseparabilidade dos efeitos nefastos (como o vício biológico) dos diversos positivos. Lembrando que, para Ellul, não há o que se falar sobre possibilidade do mal uso da internet, porque a internet não é má, nem boa, nem neutra. Não há como existir internet sem interações entre as pessoas e não há como haver estas interações sem haver problemas e pessoas tentando tirar vantagem uma da outra. Pensar todos problemas da rede poderiam ser resolvidos com educação ou com boas morais para a sociedade é ser um inocente útil para a técnica. Lembremos que os CEOs de empresas da tecnologia não dão sem restrições pros seus filhos o que eles mesmos produzem.

A internet aliena o homem de tantas formas. Na cultura, aliena o homem a ter que conhecer a cultura que lhe é imposta – e não só disponibilizada para que, com “liberdade de escolha”, o usuário consuma – como memes, posts, saber o que certa celebridade fez, saber nomes e histórias de filmes e séries famosas, atualizar-se dos resultados de jogos, enfim, estar antenado no que o mundo anda aprontando. Não estar na internet é ser desatualizado e a maioria dos seres humanos tem medo de ser taxado como ultrapassado. No trabalho, a especialização o leva a desconhecer todo o resto e se ele não se encontra nas redes sociais, dificilmente angariará novos clientes. Em sua mentalidade, o ser humano joga fora suas morais e espiritualidades e troca pelo normal ou comum, por aquilo que todo mundo é e faz, se adapta e se cancela para não ser cancelado. Somos levados a construir uma autoimagem positiva e artificial que busca admiração por nossos (des)conhecidos, pelo desespero do (mal) julgamento. A alienação da rede o faz buscar coisas que aparentemente lhe trariam felicidade, mas ele foi induzido a buscar

tais confortos e mercadorias. Aliás, a cultura hoje é mercadoria, é consumo e nada mais. Cultura é vendida e comercializada, é consumida e, só depois, experimentada e, logo após, descartada. O modelo padrão do que não é bom é aquilo que foi pouco consumido por poucos. Se uma maioria não quis certa cultura ou mercadoria, provavelmente quer dizer que ela não é boa. Parece democrático, mas são apenas aparências. Porque o que é considerado bom ou cultural na rede já foi modificada e propagada pela técnica. Até o sexo foi alienado na rede a um mero objeto de consumo com os sites pornográficos. Sexo nos é até estimulado com propagandas, filmes e séries com atores no padrão de beleza sexy e ações cotidianas erotizadas.

Quando deixamos de ser algo por medo de julgamentos e não por poder causar algum mal a outrem, acabamos por nos aderir a uma massa a fim de evitar aborrecimentos e conflitos. Quando perdemos nossos valores ideológicos e morais, ganhamos os novos valores de racionalidade técnica. Estarmos inseridos na “sociedade da informação” e na “sociedade do conhecimento” parece um progresso de nossa espécie, mas trata-se de um fracasso das individualidades. Cada vez mais, na rede, será difícil sermos nós mesmos, sermos verdadeiramente livres. Mas veja, seria a internet, então, uma inteligência artificial avançada que nos vicia e condiciona a ficarmos na rede? Não. Ela é um evento e um objeto inanimado e, portanto, sem finalidade. A internet pode ser usada para comunicar, mas este é seu uso-meio e não seu fim. Nunca saberemos precisamente todos os efeitos da rede em nós, principalmente porque nela estamos inseridos como julgador e vítima. Como milhões, bilhões, trilhões de interações, trocas de informações, dados e bytes na rede, como poderíamos prever os efeitos produzidos pela rede em nós, inclusive em nível inconsciente?

Sobre estas características da técnica em relação aos dados pessoais: no seu automatismo, temos a impossibilidade de se recusar o método mais eficaz de lidar com os dados pessoais quanto ao armazenamento inquestionável e desenfreado de dados nas imensas redes de servidores de armazenamento; no seu autocrescimento, vemos a técnica de tratamento de dados produzindo a si própria, por exemplo, os dados são traduzidos em algoritmos e *bytes*, suscitando problemas de natureza técnica que exigem soluções que só a própria técnica pode resolver, como a utilização de mais processos de criptografia, mecanismos que impedem o mau uso por cibercriminosos de brechas, e de tecnologias de aumento de armazenamento; já na sua unicidade, é indiferente o dado e o uso que dele se faz, ou seja, o dado pessoal é só aquele que tem alguma utilidade e que é, portanto, tratável; no seu universalismo, observamos a perda de privacidade pela obrigação técnica de que todo dado tem que ser tratado e os países ou empresas que não o fazem estão perdendo este potencial econômico e ficando atrás de seus concorrentes, sendo até questão de sobrevivência mercantil explorá-los; na sua autonomia, a técnica de

tratamento de dados não aceita ser julgada, tanto que questões éticas e morais são vistas como antieconômicas e, logo, antijurídicas, justificando qualquer tratamento como consequência e necessidade inevitáveis que “a sociedade impõe”, mas é a técnica que racionalmente apropria de tudo palpável; na sua ambivalência, já citamos a inseparabilidade dos benefícios com os potenciais malefícios, não há como tratar dados sem o perigo do *data breach* e do mal tratamento; na sua alienação, a técnica deturpa a realidade humana, domina nossas atividade e nos traduz em dados e imagens que definem muitas vezes quem somos; na sua misantropia, quando a técnica opta pela eliminação de tudo o que não é técnico e, portanto, humano, como nossas morais, éticas e mentalidades, a numeração e quantificação do ser humano em dados cada vez mais nos inumaniza e condiciona a comportamentos padronizados; na sua falta de finalidade, a “vontade” de que tudo seja o mais eficaz possível é o meio para um fim desconhecido, a quantificação não pode ter como fim a felicidade coletiva humana porque não existe escolha de refutá-la através de nossas interpretações subjetivas da realidade, vontades e paixões e como serve à nossa felicidade se podemos não refutar esta coleta e tratamento?; e, por fim, com efeitos imprevisíveis, pois mesmo havendo as consequências esperadas (receber *ads* mais personalizados) e previsíveis (como *data breaches*), há também as imprevisíveis, como nossa alienação, o impacto psicomental no ser humano, a aleatoriedade para onde e para quem os dados irão após serem compartilhados ou furtados e como eles serão utilizados contra o usuário.

Tais fatos podem ser considerados malefícios da internet e vejamos que Ellul sabia desde sempre que há também confortos e benefícios que técnicas e tecnologias nos fornecem. Através do acesso à internet, o indivíduo participa da sociedade e do Estado. Além de se comunicar, o indivíduo se expressa, se informa, utiliza serviços públicos, conhece mais e acessa determinados produtos e serviços oferecidos pelo setor bancário e comércio eletrônico. Através da rede, tem-se o ensino à distância – e aquele informal por meio de vídeos de YouTube ou textos do Wikipédia –, o teletrabalho e a virtualização do relacionamento social. A digitalização de aspectos da cidadania não substitui, mas complementa a justiça social, por exemplo, com a TV Justiça. Modernizou-se atos processuais (certificação digital, despacho judicial via SMS), na virtualização de audiências (interrogatório por videoconferência) e, mais recentemente, na veiculação online das audiências do STF pelo portal “JusTube”. Ou seja, tornou o processo mais célere, mesmo que também o deixou com decisões ainda mais padronizadas. Diria Ellul ser isso culpa da ambivalência da técnica. A informatização permite, sem supressão de outras garantias ou fases processuais, segurança aos autos (que são digitalizados em diversas cópias em vários dispositivos), facilidade (pode ser acessado em qualquer localidade) e desoneração

no acesso (as partes e advogados não precisam se deslocar e não há necessidade de um serventuário para atendê-los em que só uma parte de cada vez pode obter os autos), além de comodidade e rapidez no fluxo de informações, evitando deslocamento de recursos materiais (como viaturas) e humanos (como agentes penitenciários e policiais para transportar o indiciado até o julgamento).

Como aspectos negativos, podemos citar que a superexposição do Poder Judiciário foi um dos motivos do atual redimensionamento da postura dos ministros do STF. Essas transmissões, sem cortes e na íntegra, atrapalham a espontaneidade dos ministros, culminam em suas superexposições e acabam servindo também para a promoção pessoal dos mesmos, além de advogados e ativistas. Todavia, a crítica e exposição destas decisões ainda são o caminho mais democrático e benéfico para a sociedade. Como a democracia deve se renovar, a internet pode servir como plataforma de emancipação social.

Ellul alegaria que a internet é uma técnica perigosa, mas a cada benefício que se constata da internet, se torna mais complicado vislumbrar seu custo benefício como ruim.

### 3.2.1 Sacralização da Imagem e Banalização Da Palavra

*Nos esforçamos para correspondermos a padrões de regularidade, de homogeneização de condutas e da supressão de subjetividades.*

Hoje em dia, é latente o risco da manipulação de uma imagem, com recursos de softwares, especialmente em revistas e na internet que circulam fotos de celebridades sempre manipuladas, pois precisam parecer perfeitas aos olhos do espectador, quase sempre com o uso de *photoshop*, um software que edita e cria imagens ou adiciona algum efeito especial. Mas como podem as palavras – frutos de percepções subjetivas de uma pessoa – ser mais confiável que a imagem? Se uma imagem pode ser alterada, as palavras com seus problemas de interpretação podem ser ainda mais manipuladas. A utilidade dessa ideia de Ellul é a inquestionabilidade do ser humano, porém a sacralização da palavra não seria melhor que a da imagem. Antigamente, inclusive, havia bastante sacralização da palavra no meio científico-acadêmico e na doutrinação religiosa, utilizando-se dos argumentos de autoridade. A moral da conclusão, do silogismo da premissa maior “somos levados pela técnica a autosabotarmo-nos” e de premissa menor “a imagem é manipulável e incontestável hoje em dia”, é a de que não devemos sacralizar nenhum dos dois e sim considerar todos os fatos com cautela nas

interpretações e jamais devemos levarmo-nos a inquestionáveis conclusões. Mas notemos: nunca na História se questionou tanto tudo possível. Mesmo com recorrentes ignorâncias intelectuais, não estamos atrás de nenhum momento. Mesmo com as atuais conformações, antigamente eram em maior escala. De fato, quanto mais avançada uma tecnologia, mais projeções de imagens capazes de constituir uma irreabilidade alienante que retira do sujeito qualquer possibilidade de escolha e crítica. Facilitadores e confortos modernos retiram a autocritica pela técnica de proteção ao seu frágil ego o qual palavras podem colocar em xeque através da crítica subjetiva.

A internet como indústria cultural é o principal meio de socialização e integração do indivíduo na coletividade, por meio da renúncia de sua individualidade. Seu potencial de alienação é imenso porque suas projeções constantes de imagens impossibilitam a reflexão. E, como vimos na História, sempre houve este processo de transformação do eu em coletividade. Na maioria das vezes foi através do Estado e em outras através de convenções sociais, como o que se vestir ou se preocupar política ou espiritualmente, com variedades de religião. O ser humano sempre buscou – talvez porque a coletividade impôs a ele – estas projeções para além de si próprio, o que mudam são as formas. Por isso, há a moral elluliana de que a indústria cultural seria um mal a se combater, com tantos outros milhares de fatores sociais que também condicionam o indivíduo. E a moral que propomos é a de que deve ser combatida toda e qualquer falta de questionamento sobre todas conformidades, como existe na indústria cultural.

Depois do consumo, nos esforçamos para correspondermos a padrões de regularidade de condutas e de supressão de subjetividades. Um exemplo emblemático desse mundo da teatralização da vida – até na Grécia Antiga havia a peça dramática, trágica ou cômica – são os programas de *reality shows*, um gênero de programa de televisão “baseado na vida real” cujos acontecimentos nele retratados são visados da história de pessoas reais e não personagens, que transportam o espectador para a tela, tornando-o parte de um espetáculo. Anualmente, programas como o “Big Brother Brasil” ou “A Fazenda” entorpecem brasileiros de seus problemas pessoais. Ao assistirmos a teatralidade artificial – que representação não é artificial? –, visionamos um fato como se dele fôssemos partícipes. Nesse sentido, a alienação nos desmobiliza, fazendo-nos acreditar que “eu vi, portanto eu agi” (LEITE, 2012, p. 183-198).

Nos alienamos pela admiração ao artificial porque nele tudo podemos, enquanto na realidade somos limitados e frustrados. Esta realidade-artificial desejada teve, na História, outras facetas, como sonhos, crenças, religiões e medos. O ser humano sempre teve meios de se alienar. A grande questão é em que medida o ser humano escolhe estar nesse anestesiamento da realidade e em que medida é imposta. Parece que queremos nos alienar; outrora, os meios –

seja eles estatais, empresariais, artificiais, tecnológicos ou técnicos – nos condicionam. Por isso, o estudo de Ellul é muito importante para reconhecer esta dualidade e buscar alterar o poder destes meios sobre nós.

Assim como as palavras, as imagens podem ser manipuladas por pessoas e muitas vezes tem conotações de conspirações, porque não há evidências. No Brasil, temos a emblemática relação dos espectadores com as telenovelas e com a assimilação dos personagens como pessoas reais com tramas que passam a ocupar boa parte de suas preocupações. Na internet, posts e vídeos do que falam e fazem artistas e (sub)celebridades são a nova fonte de entorpecimento social. Outro exemplo global são as viralizadas séries que, assim como qualquer outra construção da realidade, produzem para o espectador uma explicação satisfatória e simplificada. As tramas de séries e filmes são quase previsíveis sempre, afinal, não pode ser intenção do cineasta ou do roteirista fazer o espectador questionar sua inteligência. O conteúdo digital tem que ser consumível por todas espécies de espectador. Assim, como no caso da TV, Ellul preocupar-se-ia com a falsa promessa de reposição libidinal pela efemeridade e fugacidade de projeções da internet (LEITE, 2012, p. 183-198). A fuga pela internet e TV muitas vezes serve para o esquecimento momentâneo da realidade, assemelhando-se às peças gregas, ao “pão e circo” de Roma, às peças ao ar vivo em toda Europa por séculos, aos teatros shakespearianos, às apresentações de cantos populares e aos livros que serviam muitas vezes para este refúgio. Todavia, não há parece haver diferença na fuga de livros em comparação à TV e à internet, se não na forma. Em ambas, a indústria cultural cria uma falsa sensação de realização e pertencimento para o sujeito. Muito similar com a satisfação, artificialmente criada, de torcer para um atleta, time ou seleção de qualquer esporte.

A imagem transmite informações como evidência e nos leva a uma convicção acrítica. Todos problemas que a imagem possa ter, o discurso os tem de maneira mais agravada. Afinal, por exemplo, confiar mais em uma testemunha do que em outras evidências como um vídeo em alta resolução, colocaria qualquer pessoa em perigo às vontades alheias. E este discurso parmenidiano de desconfiança dos sentidos não traz mais confiança ao conhecimento produzido pela palavra em relação àquela produzida pela imagem. Devemos questionar tudo, não sacralizando qualquer espécie de evidência, fazendo das nossas considerações as melhores possíveis com os fatos e meios disponíveis. É necessário atentarmo-nos à influência deste visual construído na nossa vida. Assim, notemos que a imagem nos aliena apenas quando se vende como transmissão do real e não como reconstituição fictícia da realidade.

### 3.2.2 Propaganda e Publicidade como Alienadoras a Serviço da Técnica

*Informação e propaganda não podem ser separadas.*

A propaganda é uma atividade humana muito antiga, podendo ser encontrada até em autores romanos como Tito Lívio. O termo em si surgiu no seio da Sagrada Congregação Católica Romana para a Propagação da Fé, uma comissão de cardeais encarregada das missões estrangeiras da Igreja Católica. A propaganda hodierna é um tipo de técnica do homem que põe em ação técnicas de massas mecânico-eletrônicas (imprensa, rádio, TV e internet) que são meios diretos de comunicação com pessoas e que, ao mesmo tempo, atingem o ser humano utilizando-se do poder de persuasão e de pressão psíquica. A propaganda serviu e ainda serve para convencer o receptor de algo intencionalmente a fim de induzi-lo a agir de certa maneira, como comprar algo, seguir certa religião ou militar por certa ideia. Essa técnica presta diversão, política e consumo, enfim, informa e convence. Assim, nenhuma informação é puramente objetiva, especialmente a transmitida pela propaganda. Um exemplo foi a forma com que países convenceram seus homens a participar de guerras sem se sentir presentes nela, como os EUA faziam e fazem hoje muito bem, fundada no patriotismo contra o terrorismo; há também o clássico exemplo da propaganda nazista, majoritariamente contra judeus e socialistas; e a do socialismo, contra nazistas e o capitalismo. Ou seja, a propaganda tem uma ação muito parecida com a da técnica: seus meios assumem tal magnitude que o homem nem percebe que está sendo convencido.

Com a globalização do presente século XXI, os valores humanos são levados, através da propaganda, à produção de um sentido (artificial) para a sua existência através do apelo sexual ou até do ressentimento e do ódio, apontando adversários como autores de todos males como fizeram os nazistas com o judeu e os comunistas com o burguês, explorando a necessidade latente em cada indivíduo de ter um bode expiatório para o fracasso de sua autodeterminação. Na psicologia, esta necessidade é chamada de autossabotagem. Resta aqui evidente o poder destruidor dessas manipulações. Não é possível discernir e identificar inteiramente estes malefícios já que ainda estão em funcionamento em nós e são sempre recentes demais para observarmos suas verdadeiras consequências. É difícil que um só homem identifique e tenha cuidado com tudo aquilo que busca defini-lo em sua essência, pelo contexto em que se insere, quem dirá uma sociedade inteira ter cuidado suficiente com cada propaganda que poderá defini-la em algum sentido.

O grande problema da propaganda é o mesmo da técnica ou do Estado ou do (liberalismo de) mercado: ações individuais podem atingir indiretamente o coletivo e formar conformidades passivas de contextos ruins para a sociedade, gerando uma cultura misógina ou racista por exemplo. No atual mundo, o homem tem mais contato com o artificial – em parte estimulado pela propaganda – do que com o natural. O artificial é seu novo quadro natural. A propaganda, assim como qualquer meio técnico, é fruto da natureza humana de tentar encontrar sentido no mundo. No repasse por vários meios e interlocutores, a informação hoje rapidamente perde sua fonte e, logo, sua credibilidade. A informação compartilhada nunca é neutra pois é abstraída pelos juízos de valor do locutor. Como na técnica, resta difícil – para Ellul, impossível – manter só a natureza de honestidade e transparência da propaganda perante as intenções do interlocutor, porque mesmo a ideia mais justa é propagada. Ellul mostra que informação e propaganda não conseguem ser separadas. Se fôssemos resumir todas preocupações de Ellul a uma frase seria: o grande poder alienador, que desfavorece a reflexão crítica, de técnicas no ser humano que impede seu direito de autodeterminar-se. Uma falta de (auto)crítica só pode beneficiar um terceiro e, para Ellul, este é a técnica, onde somos guiados por estes elementos inconscientes e artificiais com intenções alheias às nossas. Estes elementos inconscientes são as técnicas, tecnologias, é o Estado, empresas, outros indivíduos, ideologias, enfim, tudo aquilo que nos influencia sem nosso bem querer. Ellul quer que tomemos consciência dos elementos que antidemocraticamente nos influencia, sendo a técnica seu principal foco. E uma das técnicas mais claras neste sentido é a propaganda, política ou comercial (publicidade), como um eficaz instrumento de alienação, ou seja, de indução de comportamento inconsciente.

Adaptar é uma conformação rotineira biológica, que muitas vezes não advém de um sentimento maquiavélico de uma técnica como a propaganda, ela pode estar no instinto de sobrevivência, de querer conformar adaptativamente com o meio ou de assemelhar-se à maioria para não chamar atenção, pois suas diferenças podem indicar alguma espécie de fraqueza ou ignorância. Todos estes instintos são observados pela biologia em qualquer coletivo animal. É normal tanto para o homem-animal quanto para o homem-racional. A reação à desconformidade do grupo é encontrada quando o alfa repreende um rebelde do bando ou a beta ensina seu filhote a comportar-se. Mas o que é o melhor para o grupo? Só porque é tradição, deve haver concordância? Animais não têm consciência nem a mesma racionalidade de causas e efeitos de seres humanos. Portanto, devemos questionar tudo aquilo que nos impede, especialmente quando algo deslegitima e até banaliza seu (re)agir contra. Esta luta contra a banalização tem de ser frutífera, não relativizando completamente o conhecimento consolidado sem evidências de outra realidade palpável, como fazem terraplanistas.

Ellul defendeu “Diretivas para um manifesto personalista” (ELLUL; CHARBONNEAU, 2011) para que tivéssemos uma vida equilibrada material e espiritualmente e uma destas diretivas tratar-se-ia do combate à alienação da publicidade. Com igual problema à ideia de Marx (1867), quem controlaria o que seria essa vida equilibrada material e espiritualmente e quem fiscalizaria ou até encerraria esta publicidade ou qualquer outro meio comunicativo para consolidar tal vida? Alguém teria de tomar tal decisão subjetiva. Aliás, como comunicar ao outro sobre como esta vida é e como deve ser alcançada se não por propaganda? Propagar informação, nem que seja em uma mera conversa, com a intenção de convencimento é propaganda. A inocência de Ellul em particular se revela no combate à publicidade por ser “sua influência nefasta do ponto de vista moral, sua esterilidade de gastos econômicos, sua importância na criação de um falso ideal de vida” e porque a “única forma de publicidade normal deve ser feita por cartazes sem comentários e o anúncio, e passar pelas mãos do governo” (ELLUL; CHARBONNEAU, 2011, p. 166). Mas, ao mesmo tempo, Ellul cita casos em que o próprio Estado foi o vilão da propaganda – como nos EUA, na Alemanha Nazista ou na URSS socialista – e sabe que o Estado pode permitir tão somente aquelas que beneficiam certa vertente política vigente. A realidade nos mostra que a solução não é cessá-las e sim torná-las mais claras e identificáveis ao receptor ou informá-lo de sempre ser crítico às informações que chegam a ele.

Destarte, Ellul não tem sucesso em suas soluções, mas acerta nas críticas sobre a imposta realidade e a alienação pela ambivalência. Sobre as publicidades, Ellul observa que terão caráter persuasivo e objetivarão massificar o consumidor, merecendo atenção especial àquelas que enganam – como dizer que um produto é melhor enquanto é, no máximo, diferente – através do convencimento inconsciente. De acordo com Garcia (2011), temos as seguintes técnicas: publicidade oculta, sendo aquela que esconde seu caráter publicitário, se apresentando como informação neutra e desinteressada; publicidade *teaser*, que despertam a expectativa e a curiosidade do consumidor pelo aumento de interesse na divulgação do produto; publicidade em tom de exagero, que exagera para chamar a atenção; publicidade excludente, que transmite a impressão de que a empresa, o produto ou serviço anunciado são os únicos (bons) no segmento; publicidade testemunhal, quando uma celebridade, um especialista ou mesmo o consumidor dá o seu testemunho pois juízos de terceiros têm mais credibilidade do que as dos anunciantes; e a publicidade comparativa, que mostram vantagens em se optar pelos serviços do anunciante.

Para muitos, a solução está no controle do conteúdo e da veiculação publicitária. A publicidade sempre deve ser explícita, fundamentada e não enganosa. Porém, no ciberespaço

onde redes de anúncios monitoram os usuários, constituem-se uma publicidade invasiva. Com a LGPD, o implemento do uso de Cookies forneceu certa “escolha” pelo usuário se quer ou não tão recolhimento de dados por websites e aplicativos. Mas tudo pode quando o usuário clica em “Concordo”? O Direito deve combater a publicidade que, aproveitando-se da dificuldade de percepção pelo consumidor do conteúdo publicitário ou da falta de outra opção viável, busca a consequente maior alienação do indivíduo pela propaganda inevitável. Nota-se que, hoje, informar, comunicar ou propagar são a mesma coisa, são inteiramente a mesma ação humana nas redes.

### 3.2.3 Tecnificação e Massificação da Humanidade

*O homem fica escravo do que uma vez foi seu remédio.*

A tecnificação da humanidade pela massificação da aparência e da personalidade psíquica não se dá somente pela propaganda, ocorre em diversas formas como através da banalização da palavra e da sacralização da imagem. Pode-se somar todas técnicas hodiernas porque todas levam a este fatídico meio-fim. A racionalidade técnica demanda a transformação do meio real em artificial (o urbano e os concretos), tornando-se crucial a artificialização do próprio ser humano para que a vida não perdesse o seu sentido natural, como vimos. A criação dessa sociedade artificial, portanto inumana, pela técnica desencadeia no ser humano um vazio pela perda de sua individualidade física, psicológica e “espiritual” para a uniformidade de massa que refaz a personalidade e aparência humana à sua imagem.

O problema visto por Ellul não é a lógica de mediação da imagem com o real que cria uma realidade falsa, mas sim o efeito nefasto no homem pois, inconscientemente, este não enxerga as consequências que gera com o tempo, valorizando a imagem tão quão a própria realidade. Um desses malefícios é o mergulho na realidade falsa que ausenta o homem de si mesmo, o tornando vazio e tecnicizado. Outro é o estilo de vida que não se funda mais em valores éticos e sim em necessidades artificialmente criadas e manipuladas para que escolhamos algum produto ou serviço de uma empresa, Estado ou indivíduo. Tanto que nossos gestos não têm mais o direito de exprimir nossa personalidade, eles devem exprimir alguma cultura já concebida. Nossos gestos e “nosso eu” só têm reconhecimento quando inseridos em algum contexto socialmente aceito, inclusive há imposição cultural até dos próprios povos historicamente oprimidos como negros, indígenas ou judeus ter de honrar seu passado vestindo-

se de acordo e relembrando lutas passadas. Mesmo que a pessoa se considere anárquica ou tenha uma cultura antipadrões, ela adere-se a um padrão já pré-estabelecido. Aliás, o maior estilo de vestimentas vendido hoje é o do jovem que “busca ser diferente do padrão do subúrbio”, com estampados de frases empoderadoras ou com símbolos de revolta social, vestimentas folgadas ou rasgadas e penteados largados, no estilo hippie.

Foi explicado no presente trabalho a constante retirada de características individuais e conscientes da personalidade humana, a chamamos de misantropia. O perigo das técnicas reativas é que buscam produzir um reflexo condicionado pela provocação de comportamentos padronizados que modificam quem somos. Como saber se é para o mal ou para o bem? Se estes reflexos nos levam a morais ou ações boas, não importa para a técnica e, por isso, importa para o estudo dessa dissertação. A Psicologia categoriza as emoções básicas em felicidade, surpresa, raiva, tristeza, medo e repugnância. Notemos como a propaganda ou a simples informação veiculada na internet pode instigar em todos estas emoções, modificando-nos. Vejamos exemplos. Quanto à felicidade, é clássica a associação de que um produto trará felicidade; à surpresa, temos os *clickbait*s, uma forma de anúncio falso a fim de atrair a atenção e motivar os usuários a clicarem no link com informações tipicamente sensacionalistas ou enganosas, que utiliza-se de notícias sensacionalistas para obter mais acessos; à raiva, de grupos políticos se utilizam da crença generalizante de que todos do tipo contrário a eles devem ser combatidos; à tristeza, da indução de comportamento parecido ao da felicidade: caso não tenha ou não faça de acordo com a propaganda, o indivíduo se tornará incompleto e, logo, infeliz; ao medo, de Estados que utilizam de propagandas – aqui no seu sentido original – sobre outros países para apoiar suas ações; à repugnância, geralmente associa-se a outra como medo ou raiva, do indivíduo passar a repugnar certo pensamento, pessoa ou país porque fizeram algo que merecesse já que seus motivos aparentemente foram insuficientes; quanto à simpatia e compaixão, podemos acompanhá-las em campanhas da Cruz Vermelha ou de ONGs que atuam na África, pedindo doações online através de vídeos com pessoas em estado de necessidade; o embaraço e vergonha estão, por exemplo, em propagandas de produtos de limpeza de roupa para indicar que estar com uma roupa não tão limpa ou manchada é embaraçoso (mesmo que custe a mais ao consumidor mais carentes ter que pagar por estes produtos); a culpa é clássica nas propagandas ou informações parciais que culpam a inércia da pessoa por certo fato (ao atingir negativamente terceiro), induzindo a mudança de comportamento (a adquirir algo) a fim de evitar este fato: como o convencimento do uso de certa marca por ser menos danosa ecologicamente; no orgulho, podemos citar o, também clássico, uso de uma marca imponente e que impõe respeito social, como as propagandas de carros de luxo; ciúme e inveja são mais

difíceis de serem propositalmente instigadas (pela dificuldade de se extrair valor), mas ocorre nos discursos de que países estão melhores por causa de certo fator parcial, como ter mais universidades privadas em que liberais propagam como fator decisivo ou colaborador e que, por isso, também deveríamos adotar; a gratidão e admiração coexiste bastante no mundo da música, onde um artista busca convencer seus fãs a comprar seus discos (e não só baixar suas músicas gratuitamente) como forma de compensação e de estímulo para que este possa continuar seu trabalho; e o espanto, a indignação e o desprezo podem ser encontrados em qualquer propaganda ou informação que estimule um comportamento contrário àquele que causa um evento ruim.

Toda escolha envolve política e ideologia, até mesmo os bens de consumo envolvem um juízo de valor. Como exposto, toda escolha que envolva qualquer propaganda ou informação apresenta em *ultima ratio* uma questão de juízo de valor, não se subsumindo meramente ao conhecimento racional e sim interagindo com o fator emoção. Não cabe, portanto, a ideia de que a propaganda serve tão somente para que o consumidor conheça os fatos para tomar a melhor decisão ou que serve para ajudar na decisão final, pois elas impõem seu argumento.

O ciclo vicioso, de reforços positivos ou negativos, da propaganda e da publicidade trabalham sobre o mecanismo de compensação, não se importando com as nocivas e imprevisíveis consequências no sistema de equilíbrio do inconsciente humano. Nosso reducionismo ao que deveríamos ser é notado na política nos EUA, no jogo entre Republicanos e Democratas; vê-se também no Brasil das últimas duas décadas: a chamada direita, representada pelo PSDB, e a intitulada esquerda, representada pelo PT. Veja que temos poucas verdadeiras escolhas: ou somos de direita, de esquerda ou de centrão. Mas nem tudo está perdido, há várias atitudes que desafiam as tendências técnicas. Por exemplo, movimentos feministas conseguiram reduzir bastante a objetificação do corpo feminino em propagandas consideradas machistas. Lembremos o sistema de comunicação digital pode melhorar a vida de pessoas e o desenvolvimento da ciência, da tecnologia, do comércio, da indústria, das artes, para a defesa dos Direitos Humanos. A chamada Primavera Árabe começou pelo Twitter. As redes sociais e os demais recursos da internet trazem potencialmente inúmeros benefícios, mas também nos aliena a outros inúmeros malefícios.

### 3.3 GLOBALIZAÇÃO DA INTERNET, NECESSIDADE DE CONSTITUIÇÕES CIVIS

## TRANSNACIONAIS E PROBLEMAS TRANSFRONTEIRIÇOS

*A internet carece de ser regulamentada como necessidade global.*

O presente capítulo explicará a abordagem tão necessária do Direito Digital como uma essencial pretensão jurídica global, de forma integrada, não a partir da propositura de mecanismos legislativos tão somente nacionais, mas expondo um complexo sistema de regulamentação deste direito em espaços globais, inclusive diante dos atores sociais que reclamam inovadoras maneiras de proteção dos bens jurídicos. Não é possível combater o crime organizado internacional sem uma coordenação conjunta de países e instituições investigativas e, igualmente, não é possível resolver todos problemas transfronteiriços da internet somente com ações nacionais.

A resolução das adversidades apresentadas por esta organização interativa e informativa transnacional, chamada de internet, antecede as relações institucionais em nível global. Lembrando que a Convenção de Budapeste atua mais como uma referência e arcabouço de princípios, uma espécie de Constituição, havendo ainda a necessidade de uma pretensão jurídica global específica e integrada para a devida regulamentação deste ator social. Esta pretensão deve se destinar ao bem-estar social e à concretização dos direitos fundamentais, especialmente a liberdade e privacidade, e da dignidade da pessoa humana como valores essenciais de permanente justificação do Estado Democrático de Direito.

Os direitos fundamentais, numa abordagem internacional, possuem eficácia horizontal também entre atores privados, indivíduos e empresas. Dessa forma, como prevê Teubner (2003, p. 4), as obrigações fundamentais alcançam as relações privadas transnacionais, ao mesmo tempo em que elas são possíveis de serem perseguidas em espaços como a internet. A noção de multiplicidade de Constituições Civas é defendida por Teubner como uma forma de superação dos problemas de âmbito mais internacional. É uma nova racionalidade constitucional sustentada em uma constatação tríplice (TEUBNER, 2003, p. 7-13).

A primeira parte desta tríplice trata do Dilema da Racionalização, onde a Constituição seria construtora de uma unidade de diferença. Enquanto a Constituição não se adaptar a essa realidade, ela será uma diferença para promover a unidade, algo que pode ser classificado, no mínimo, como anacrônico já que o câmbio de uma sociedade moderna para uma sociedade de risco expõe a fragilidade das modernas estruturas da sociedade de indeterminação. Perigo que ocorre em maior escala na dinâmica internet, com novos tipos de cibercrimes e *malwares*, onde a centralização se esgota em algum momento. A segunda é a Globalização Policêntrica, pois a

sociedade civil tem níveis variados e não coordenados, reafirmando a Constituição em espaços fora e dentro do Estado, constituindo a ideia da Constituição Civil a ser transplantada a um nível global, medida que parece ser necessária ao se tratar do mundo real-virtual. Já o *Creeping Constitutionalization* se refere aos países de modernidade tardia que vivem sob o manto de uma baixa constitucionalidade, como no Brasil onde inexistente diferenciação entre Direito e Política, o que provoca bloqueios na necessária autopoiese de ambos os sistemas. A consequência direta é uma ausência de constitucionalização do sistema jurídico e, portanto, de uma *Creeping Constitutionalization* em países periféricos. A Constituição, pois, é vista sob dois aspectos: o espaço de produção de normas e de fundamentação do Direito. Separar o lado jurídico do político é de extrema importância já que qualquer descuido pode significar alguma medida desproporcional ou autoritária por parte do Estado.

A proposta de Teubner (2003, p. 16) é a de que as várias Constituições (Cíveis) sem Estado são estruturas sociais de movimentos sociais autônomos com as operações juridificadas. A Constituição não seria somente o acoplamento entre Direito e Política, mas sim entre o Direito e os demais subsistemas sociais. Assim sendo, a Constituição não é tão-somente política, muito embora ainda preserve tal característica. De outros subsistemas provém irritações que podem ser entendidas como constitucionais pelo sistema jurídico. Para Teubner (1997, p. 769), não se pode mais silenciar o erro da hierarquia constitucional já que as dúvidas recorrentes sobre a hierarquia da lei tão facilmente silenciadas no passado dos estados-nações não podem mais ser silenciadas. Por exemplo, nas Cortes de Arbitragem Internacionais, as empresas multinacionais aplicam, em um local fora do Estado, leis comerciais que são internacionais e cuja reflexividade no sistema social não pode ser desconsiderada.

É a ideia de “aldeias jurídicas globais” nas suas relações com os respectivos sistemas sociais globais: sobressai a instrumentalização das ordens jurídicas mundiais por outros âmbitos de comunicação da sociedade mundial, como uma *lex digitalis* para a internet. É uma questão que envolve os direitos humanos. Marcelo Neves menciona que talvez não seja o mais apropriado definir estas formas de relação entre ordens jurídicas transnacionais e os correspondentes sistemas funcionais globais como “Constituições Cíveis” (NEVES, 2009, p. 111). O autor prefere a melhor adequação de entrelaçamento de ordens jurídicas no âmbito do transconstitucionalismo, porém, sem mencionar maiores ferramentas práticas desta teoria.

A internet, neste norte, carece de ser regulamentada como necessidade global. Por sua vez, em espaços cada vez mais tomados pela globalização e suas múltiplas facetas, a demanda que se apresenta não pode ser limitada aos limites fronteiriços estaduais e/ou blocos

comunitários. Ao tempo em que o problema constrange o mundo, o mundo deve dedicar todos os esforços para o tratamento da crise da epidemia de cibercrimes.

Por essas razões, deste objetivo não pode se furtar o Direito global, justamente pelas diretas relações com práticas de globalização dos riscos e das pretensões jurídicas de contenção, e pelos problemas jurisdicionais os quais apresentam muitos problemas mediante a inexistência de fronteiras na internet. Problemas globais devem necessariamente ser sanados por ações globais, com reflexos locais, regionais, nacionais e internacionais. A GDPR é um bom exemplo de início destas soluções.

Há muitas outras ideologias, especialmente no Direito Internacional, com esta intenção de solucionar as interações decorrentes da globalização, como Habermas (2008), ou sobre os problemas de uma “governança global”, todos sinônimos da mesma coisa, como em Held e Maffetone (2016, p. 117-142). Por exemplo, McLuhan (1996) acreditava que a possibilidade de conhecer qualquer lugar do planeta levaria a tal integração a ponto de considerar que o mundo se transformaria em “aldeia global”. Todavia, a aldeia global idealizada por McLuhan ocorreu deformadamente na sociedade de risco porque a tendência mundial de sentimento de segurança é estar sendo vigiado centralizadamente. De qualquer maneira, ainda está longe a superação de que os Estados interpretem as leis internacionais que tangem o Direito Digital como *soft laws*. Por exemplo, no próprio Mercosul, os Estados não são obrigados a seguirem tudo que o grupo decidir.

Vejam os que em muitos atos ilícitos na rede, o servidor pode estar no país “1”, o terminal no país “2”, o titular do site no país “3” e o usuário afetado é domiciliado no país “4”, onde ocorre os efeitos danosos. Em outra hipótese mais radical, o usuário pode estar, no momento da ofensa, em outro país que não de seu domicílio, o “5”. Fixar a jurisdição no lugar onde se encontram os servidores que armazenam os dados, pode remeter o usuário a um outro continente, assim como no país onde está domiciliado o titular do sítio eletrônico. Isto pode levar o usuário ofendido a um país que sequer conhece a língua e tampouco podem os operadores do Direito daquela localidade mensurar o dano em face das diferenças culturais e jurídicas. Uma das principais formas adotadas hoje para evitar o máximo de dano possível ao usuário afetado é a fixação da jurisdição ser interpretada como o centro de gravidade do conflito (EUROPEAN UNION, 2011), até porque pode-se não saber a localização do servidor (UNIÃO EUROPEIA, 2012). Já em um âmbito mais prático e local, o Marco Civil da Internet não tem uma solução satisfatória às vítimas das violações que tenham seu centro de interesses no Brasil, quando o servidor, o titular do domínio ou os sítios eletrônicos não estejam localizados em território nacional. Em uma das poucas jurisprudências disponíveis, foi julgado que:

[...] quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil, aplicando-se à hipótese o disposto no artigo 88, III, do CPC. (BRASIL, 2003).

Em outra, foi julgado em um caso de consumidor que o certo é o “foro do lugar do consumidor lesado” (PARÁ, 2002). Apesar da jurisprudência ainda não ser bem formada, o MCI e a LGPD abrem a interpretação de que o brasileiro terá os efeitos em território nacional – quando, em seu país, “as informações falsas e difamatórias são livremente acessadas, causando-lhe danos no seu mundo real e territorialmente demarcado” (RIO GRANDE DO SUL, 2016) – em seu domicílio, sendo este o seu “centro de interesses”. O consumidor, na verdade, pode escolher entre ajuizar sua ação judicial no seu domicílio ou onde ocorreu o dano patrimonial ou moral (BRASIL, 2010).

Vejamos que o mais relevante nestes casos é o local dos efeitos danosos da violação dos direitos de personalidade no meio ambiente digital ou para onde as atividades do provedor de aplicações são dirigidas, especialmente quando se trata de indivíduo com alguma notoriedade em que pode haver danos fora do âmbito nacional.

Outro efeito da globalização e da adaptação social ao paradigma da (des)necessidade estatal, especialmente na internet, são os padrões de tecnologia de governança global, os *standards* como o ISO. Esta governança indireta fornece compatibilidade de padrões. Funciona como uma forma de recomendação e não de obrigação legal, o que não influencia no fato de que a maioria das empresas, especialmente as de médio e grande porte, sigam suas recomendações. A ISO é a sigla de International Organization for Standardization (Organização Internacional para Padronização), uma entidade de padronização e normatização formada por representantes de cerca de 170 países, cada um representando um organismo de normas, testes e certificação. Ela tem como objetivo principal aprovar e promover o desenvolvimento de normas internacionais, modelos de gestão de qualidade e testes e certificação de empresa e produtos. No Brasil, estas normas são compostas pela sigla NBR, sendo criadas e gerenciadas pela Associação Brasileira de Normas Técnicas (ABNT). No meio acadêmico, conhecemos a ABNT por suas normas sobre formatação de trabalhos científicos (14724, 10520, 6022, 6023, 6027, 6028, 6024, 6034 e 15287), mas ela vai muito além. No ramo empresarial, suas normas e certificações mais conhecidas são a: conjunto ABNT NBR ISO 9000 e subsequentes (9001, 9002, 9003 e 9004), considerada uma das mais importantes e conhecidas normas do mundo, com fundamentos, vocabulário e requisitos de sistemas de gestão da qualidade para o sucesso

sustentado de uma organização; conjunto ABNT NBR ISO 14000 e subsequentes (14001, 14004, 14010, 14031, 14020, 14040 e 14064), sobre sistema de gestão ambiental que propicia uma valorização dos produtos ou serviços da organização; ABNT NBR ISO 17025, voltada para comprovar que laboratórios de ensaios e de calibração tem práticas alinhadas e resultados precisos e de alta qualidade; ABNT NBR ISO 19011 e 10011, sobre as instruções para auditorias de sistemas de gestão; ABNT NBR ISO 22000, sobre condições de um sistema de gestão com o foco em assegurar a segurança de alimentos; ABNT NBR ISO 27001, uma das mais importantes para o Direito Digital, trata de boas práticas que garantem desenvolvimento de sistemas seguros de segurança da informação, com foco nos parâmetros da LGPD; ABNT NBR ISO 31000, sobre princípios e diretrizes na gestão de riscos através de um processo mais formal; ABNT NBR ISO 37001, para combate de sistemas de corrupção dentro das empresas; ABNT NBR ISO 45001, sobre sistema de gestão de saúde e segurança ocupacional; e ABNT NBR ISO 50001, sobre diretrizes que auxiliam as organizações a conseguirem uma maior eficiência energética e reduzindo as mudanças climáticas, dentre outras. Para qualquer empresa receber qualquer certificado da ISO, ela deve passar por um projeto com diversas fases, para garantir que a implementação seja feita corretamente ao se adequar às regras necessárias para obtenção do certificado. A governança indireta, que nasce de uma necessidade da carência global, é uma solução a estes problemas transfronteiriços.

### 3.4 TRANSUMANISMO E FUTURO DO HUMANO TECNOLÓGICO

*É possível o homem ser ou tornar-se algo que não é humano?*

Ellul previa o futuro nascimento de um novo homem sem consciência ou virtude:

Até hoje a adaptação tem sido produto da interação material, e tudo isso implica em frouxidão, desajuste e excesso. Mas a adaptação futura será calculada de acordo com um sistema estrito, a chamada 'biocracia': será impossível escapar desse sistema de adaptação porque ele estará articulado com tanta compreensão científica do ser humano. O indivíduo não terá mais necessidade de consciência e virtude; seu equipamento moral e mental será uma questão de decisões do biocrata. No momento, temos pouca concepção de como será esse novo homem. O técnico por sua existência nos dá uma ideia, mas imperfeita; o técnico ainda retém elementos de espontaneidade, mas podemos adivinhar o que o novo homem ganhará e o que perderá em comparação com o homem médio moderno. (ELLUL, 1964, p. 398, tradução nossa).

Este capítulo é nosso ápice de futurismo com ficção científica. O Transumanismo é um movimento que confia e estimula o uso da tecnologia (como a inteligência artificial,

nanotecnologia, nanomedicina, biotecnologia, engenharia genética, clonagem de células-tronco e transgênese) no organismo humano a fim de melhorar suas condições biológicas, expandindo as capacidades naturais do corpo humano (como melhoramentos físicos, intelectuais e psicológicos). Consequentemente, há inúmeras discussões éticas sobre o assunto, quase sempre pautadas no custo benefício entre a ação capaz de oferecer inúmeras vantagens e seus riscos e incertezas. Este estado pós-humano representaria a ultrapassagem dos limites naturais, como a retardação do envelhecimento e o investimento na saúde física e mental.

As seis principais teses de filosofia transumanista são: o cientificismo, comumente utilizado de modo pejorativo por aqueles que têm aversão à ciência e à tecnologia, é a ideia de que o espírito e os métodos da ciência deveriam ser estendidos a todos domínios intelectuais e morais da vida e proclama a adoção da metodologia científica como a melhor ferramenta de melhoria da qualidade de vida e superação das limitações físico-psicológicas do corpo humano, coletivamente estamos hoje muito próximos desta vertente; o ceticismo metodológico, comumente utilizado como sinônimo de niilismo epistemológico, ao utilizar-se da dúvida, propõe novas ideias e avalia criticamente as implicações do uso de certas tecnologias que visam a melhoria das capacidades humanas; o humanismo, conjunto de normas que busca a verdade e a justiça, advogando através de códigos morais e programas políticos que enfatizem a livre pesquisa, os direitos e o bem-estar humano para a superação dos problemas cotidianos; o agatônismo, filosofia moral que guia a busca do bem para nós mesmos e para os outros, combinando egoísmo e altruísmo e proclamando que as ações devem ser moralmente justificadas e avaliadas por suas consequências; o sistemismo, postulando que o mundo está composto por sistemas de distintos tipos (físicos, químicos, biológicos e sociais), auxiliando as ciências cognitivas (filosofia da mente, inteligência artificial e neurociência) em uma melhor compreensão dos processos mentais do cérebro humano; e, por fim, o racioempirismo, proclamando que a razão é necessária – mas não suficiente – para conhecer a realidade, devendo, portanto, se unir à experiência.

Quando falamos em evolução, lembramos de nossos ancestrais hominídeos em florestas e savanas, vivendo da caça e coleta. Entretanto, raramente lembramos que produziam artefatos técnicos para superar suas limitações biológicas. E o principal artefato técnico da atualidade é a inteligência artificial, havendo dois problemas éticos decorrentes dela: primeiro, no futuro não-tão-distante, a dificuldade de identificar diferenças significativas nas relações entre humanos e robôs; e o segundo problema, mais especulativo, sobre o que somos, se só a capacidade de realizar cópias de nossas faculdades mentais em dispositivos externos é suficiente e as decorrências éticas disto.

Em um âmbito mais prático sobre a IA, a inteligência da máquina pode ser descrita como um “*continuum* entre uma calculadora matemática e o homem bicentenário da ficção, representando uma evolução que vai da total dependência a parâmetros pré-programados até a sua total independência” (COSTA, 2019, p. 14-16). Hoje há certas decisões, inclusive jurídicas, que podem ser tomadas por computadores, por exemplo: a emissão de ordem de compra a partir da leitura do estoque; determinação do posicionamento em estantes a partir do estoque, estimado por dados anteriores; a negociação de indenizações por atraso de prestações com um interessado humano; uma porcentagem a um cliente potencial de um escritório ter sua ação acatada por certo juiz ou corte, dentre outros. Talvez estas ações fossem fáceis para alguns, mas para muitas outras pessoas estas decisões não seriam fáceis de tomar. Lembrando que ainda há falhas a serem solucionadas. Há casos de interpretações de dados por máquinas que geram injustiças, como a interpretação de pessoas com a cor de pele mais escura como mais propícias a se envolverem em infrações legais, levando a um aumento do valor de seu seguro. Outro problema que pode ocorrer é o robô não ser inicialmente programado para realizar uma infração, mas mediante seu sistema de recompensas incorretamente desenhado, poderia incentivá-lo a cometê-la. Como na exclusão de dados solicitados por pedido judicial, afinal, como constatar se a empresa intencionalmente programou a máquina para isso ou tratou-se de uma falta de estimativa dos programadores. Outro caso é a responsabilidade sobre drones ou carros autônomos, se adentrando no limiar do que é intencional e na responsabilização da empresa que utiliza ou cria um software ou produto. Lembrando que o STJ não permite a responsabilidade objetiva e absoluta, salvo o caso do Estado. De qualquer maneira, deverá se observar se o caso fortuito for interno ou externo, se é de incidência cível ou penal, dentre outras considerações.

Não entraremos nos problemas práticos sobre a possível e futura transferência de nossos cérebros biológicos para um corpo robótico, como o problema fundamental de que o cérebro precisa de um sistema biológico para interagir com o meio-ambiente, ou os problemas decorrentes da imortalidade e a superlotação da Terra ou o livre-arbítrio e reconhecimento de direitos, sem contar o problema do maior acesso a essas tecnologias por elites. O que instiga a filosofia transumanista é a erradicação de qualquer forma de sofrimento causado por doenças, pelo envelhecimento ou mesmo pela morte, ou seja, causados pela naturalidade biológica. O objetivo dela é alcançar as máximas potencialidades em termos de desenvolvimento humano.

Assim, o Transumanismo é uma classe de filosofia que busca nos guiar para uma condição pós-humana e isto é importante para ao menos termos algum tipo de ética ou moral de guia no futuro. Eles acreditam que os seres humanos podem e devem usar essas tecnologias

para tornarmo-nos “mais do que humanos”. Portanto, apoiam o reconhecimento e a proteção da liberdade cognitiva, liberdade morfológica e liberdade procriativa como as liberdades civis, de modo a garantir às pessoas a escolha de usar (ou não) tecnologias de aprimoramento humano sobre si e seus filhos (SANDBERG, 2001). É quase impossível provar que a orientação transumanista é apenas um delírio de ficção científica com tantos avanços da ciência. O humanismo basicamente busca melhorar o corpo humano, o que pode significar substituir o máximo das falhas biológicas por máquina pela retirada do orgânico.

Há também um movimento famoso chamado de 2045, fundado pelo bilionário russo Dmitry Itskov em 2011, que busca dar imortalidade aos seres humanos, transferindo suas personalidades e cérebro para um portador superior não-biológico mais avançado. Há diversos avanços deste tipo hoje, como: a abstração em imagem de sonhos em tempo real, o pensamento sendo interpretado como movimento – inicialmente, para amputados – e o pensamento interpretado em palavras (como uma tradução instantânea do pensamento).

Um exemplo dentre tantas outras previsões futurísticas e histórias fictícias que poderíamos citar é o de Hugo de Garis (2015). Ele apresenta uma visão distópica da guerra global entre partidos rivais, terráqueos e cosmistas, onde os primeiros querem parar a aquisição do robô antes que seja tarde demais e os cosmistas querem adotar a aquisição do robô pela esperança de que levará a um futuro surpreendente. Esta dicotomia destaca um conflito-chave do sistema de valores que pode vir à tona: valorizar a humanidade em sua forma tradicional vs. valorizar inteligência, crescimento, alegria e outros valores. Um tema que interessaria bastante a Ellul. Esta é só uma das histórias que tentam passar a moral se deve haver alguma limitação à tecnologia. Independentemente de previsões futuristas, como se vivemos em uma “era da escassez” ou em uma “era da abundância”, todos alertas são aos malefícios desta autotranscendência que o ser humano parece buscar. Aliás, é interessante esta passagem irônica de Jacques Ellul sobre possibilidade de gerar sentimentos a partir diretamente da artificialidade:

Nenhum de nossos sábios colocou a questão do fim de suas maravilhas. O ‘portanto’ é resolutamente ignorado. A resposta que ocorreria aos nossos contemporâneos é: pelo bem da felicidade. Infelizmente, não há mais questão disto. Um dos nossos especialistas mais conhecidos em doenças do sistema nervoso escreve: ‘Poderemos modificar as emoções, desejos do homem e pensamentos, como já fizemos de maneira rudimentar com tranquilizantes’. Será possível, de acordo com o nosso especialista, produzir uma convicção ou uma impressão de felicidade sem qualquer base real. Nosso homem da idade de ouro, portanto, será capaz de ‘felicidade’ entre as piores privações. Por que, então, nos prometer conforto, higiene, conhecimento e nutrição extraordinários se, simplesmente manipulando nosso sistema nervoso, podemos ser felizes sem eles? O último motivo escasso que poderíamos atribuir à aventura técnica desaparece, portanto, no ar através da existência da própria técnica. Mas de que adianta colocar questões de motivos? De porquês? Tudo isso deve ser obra de algum intelectual miserável que se opõe ao progresso da técnica. A atitude dos cientistas, de

qualquer forma, é clara. Técnica existe porque é técnica. A idade de ouro será porque será. Qualquer outra resposta é supérflua. (ELLUL, 1964, p. 436, tradução nossa).

Não é demasiado futurístico pensar que em breve teremos tais pílulas com a capacidade de simular sinteticamente ou estimular hormônios – da felicidade, do prazer, do relaxamento ou da recompensa – para serem tomados e sermos dopados diariamente. Aliás, muitas drogas e remédios já o fazem e a tendência é escalonar para que mais e mais pessoas tenham que tomá-las para sentirem-se mais felizes ou “mais em si”. Não é irrealista pensar que, em um futuro próximo, tenhamos a cultura de tomar algumas “pílulas da felicidade” para sermos felizes desde a hora que acordamos.

De acordo com o principal órgão sobre o transumanismo, o Humanity+ (2009), os interesses teóricos se concentram nos tópicos pós-humanos da singularidade, do risco de extinção e do carregamento da mente. São oito justificativas de suas intenções:

1. A humanidade deve ser profundamente afetada pela ciência e tecnologia no futuro para ampliar o potencial humano;
2. O potencial da humanidade ainda não foi realizado;
3. A humanidade enfrenta sérios riscos, principalmente pelo uso indevido de novas tecnologias já que nem toda mudança é progresso;
4. É necessário investir esforços de pesquisa para entender essas perspectivas a fim de construtivamente reduzir riscos e agilizar aplicativos benéficos;
5. A redução dos riscos existenciais para a preservação da vida, da saúde e da sabedoria humana devem ser perseguidos como prioridades urgentes e fortemente financiados;
6. A elaboração de políticas deve ser guiada por uma visão moral responsável e inclusiva, levando a sério as oportunidades e os riscos, preocupando-se com a dignidade de todas as pessoas;
7. Deve-se buscar o bem-estar de toda a consciência dos seres humanos e não-humanos;
8. Deve haver a liberdade de escolha aos indivíduos sobre como eles possibilitam suas vidas através de qualquer espécie de aprimoramento científico.

Dadas as incertezas, é impossível prever o futuro detalhadamente, objetivamente e com razoável confiança com base apenas nos dados disponíveis. Além de aspectos muito amplos, a melhor maneira de entender o futuro é começar uma estrutura conceitual abrangente que

preenche a lacuna entre o mundo que vemos hoje e o mundo muito diferente que poderá vir em breve.

Mas afinal, o futuro da natureza humana são os humanos melhorados ou não mais humanos? O que é o humano? O que é e como lhe fazer o bem? Que futuro os humanos, enquanto indivíduo e coletividade, devem buscar? (VILAÇA; DIAS, 2014). O debate em torno do melhoramento humano traz à tona estas questões, envolvendo a definição de conceitos básicos, especialmente de natureza humana, além dos valores que derivam dela. Como vimos, os transumanistas apostam na mudança da biologia humana como forma de melhorar o humano. Alguns bioconservadores temem a instrumentalização da biologia humana, prevendo que poderia erradicar a humanidade e seus valores mais fundamentais, como Fukuyama (2002) e Habermas (2004). A maioria dos filósofos da tecnologia também temem. Bostrom e Sandberg (2009, p. 375-416) citam a tendência de se dar preferência às coisas tidas como naturais, em detrimento das artificiais. Mas por que o natural seria preferível ou melhor que o artificial? Por exemplo, qual seria a diferença – enquanto o humano faz o custo benefício, até financeiramente – da felicidade gerada pelas pílulas daquela que muitos humanos cada vez mais menos sentem espontaneamente? Há características “boas” e “más” na natureza em geral – em coesão à ambivalência elluliana – bem como na humana, de modo que não há nada de errado em alterá-las. Há a definição de natureza humana filosoficamente dominante de ser um “conjunto de características que são comuns a todos os seres humanos e que distinguem os humanos de outros tipos de seres” (BUCHANAN, 2009, p. 142, tradução nossa), ou seja, ser humano é tão somente fazer parte da espécie *homo sapiens*. Há outros sentidos, como humano oposto de inumano – cruel e “sem coração” – e ter qualidades morais boas (PERSSON; SAVULESCU, 2010) ou a famosa definição de ser humano enquanto ser racional, diferente do ser animal. Ou ser humano é ter alguma virtude ou é simplesmente sê-lo como é, uma espécie animal dotada de maior racionalidade. Um outro modo de detectar esta natureza é através de um desvio padrão zero: quanto mais próximo da mediana dada característica estiver, mais afeita à natureza humana ela será. Esta interpretação tem o lógico problema em generalizar antagônicas e recorrentes características tipificadoras do humano como o egoísmo, preconceito, insociabilidade, crueldade, amar a descendência, (in)tolerância, sociabilidade, empatia ou apatia e moralidade. Vejamos que, para Cassirer (2001), mais que racionais, somos simbólicos, mas estariam os avanços tecnológicos nos fazendo perder nosso simbolismo, ou seja, nossa moralidade que nos faz humanos. Já para Habermas (2004), a natureza humana é constituída por características que lhe conferem vulnerabilidade e precariedade, servindo-nos de fundamento para nossas intuições morais, vínculos sociais e autocompreensão ética. Habermas preocupou-se com os limites

daquilo que denomina de eugenia positiva da natureza humana interna (do DNA), afinal, quais são as características estimuláveis? (VILAÇA; DIAS, 2014)

Enfim, estaríamos na iminência do surgimento do pós-humano? A natureza humana estaria, feliz ou infelizmente, à beira do acaso? Se natureza humana é um conceito arbitrário, parece que não estaríamos perdidos; se há traços naturais com os quais não convivemos mais na experiência humana, então sim, estaríamos desaparecendo aos poucos. E o que surge, o que se adapta ou se cria no (ou do) homem é o que? É possível o homem ser ou tornar-se algo que não é humano? Em suma, o futuro da humanidade deve permanecer cada vez mais incerto, menos determinável e, portanto, mais imprevisível (VILAÇA; DIAS, 2014).

### 3.5 COMO LIDAR COM A TÉCNICA

#### 3.5.1 Ações Preventivas

*A experiência deve ditar a prevenção.*

Como vimos, o design é uma atividade sujeita a um exame racional, na qual a criatividade também tem um papel importante. Como o design é uma forma de ação estruturada de decisões para proceder de uma certa maneira e não de outra, a criatividade diz respeito à geração dessas opções. Todavia, na prática, propostas alternativas para a realização de funções específicas são geralmente retiradas pelo desinteresse do cliente. Os requisitos funcionais, que definem a maioria dos problemas de design, não prescrevem explicitamente o que deve ser otimizado, cabendo ao engenheiro escolher até onde atendê-los. Por exemplo, uma empresa contrata a Google para divulgar sua propaganda, mas não exige o como ela deve extrair as informações por *cookies* dos seus usuários para fazer a propaganda mais direcionada. É a Google quem escolhe. A eficiência é um valor primordial, além da segurança e, mais recente, da sustentabilidade.

Ao atender ao mercado, um engenheiro enfrenta vários problemas de decisão. Por exemplo, um desempenho relativamente ruim em um critério pode ser equilibrado por um desempenho relativamente bom em outro critério. Como a ferramenta de busca de perfis que pode ajudar *stalkers*, alguém que importuna de forma insistente e obsessiva uma outra pessoa, e cibercriminosos a encontrarem e filtrarem suas vítimas e, ao mesmo tempo, ajudam amigos e usuários a se conectarem, mal aquele que valeria a pena. Ellul diria ser essa inseparabilidade

do lado ruim do bom de ambivalência da técnica. Surge assim uma tendência global chamada de “inovação responsável”, de incentivo a boas escolhas dos engenheiros. Ela é:

[...] um processo transparente e interativo pelo qual atores sociais e inovadores se tornam mutuamente receptivos uns aos outros com vista à aceitabilidade (ética), sustentabilidade e conveniência social do processo de inovação e seus produtos comercializáveis (a fim de permitir uma incorporação adequada dos avanços científicos e tecnológicos em nossa sociedade) (VON SCHOMBERG, 2011, p. 9, tradução nossa).

Aqueles que defendem uma posição contrária tendem à “inovação sem permissão”, em que experimentações com novas tecnologias devem ser permitidas exceto se houver argumentos suficientes sobre um possível e sério dano à sociedade. É o famoso embate da inovação “*by default*” ou “por padrão” e a “*by design*” ou “por design”, esta última preferida dos filósofos da tecnologia.

Na acepção de Thierer (2016), a inovação tecnológica não deve ser tratada “*by design*” por cinco motivos. Primeiro, a inovação tecnológica é o que mais determina o bem-estar humano a longo prazo e, logo, qualquer restrição que transparecesse ser moralmente boa agora, poderia acarretar em grandes prejuízos futuros. Segundamente, há um valor real para o aprendizado através da experimentação contínua de tentativa e erro na resiliência e adaptação às mudanças tecnológicas. Para a maioria dos problemas da “excessiva liberdade” de mercado, qualquer que seja o malefício, é benéfica a demonstração do erro para aprendermos a não repeti-lo e é melhor do que suprimir uma escolha que possa vir a ser um erro, pois não há uma certeza que este acontecerá enquanto poderá haver também benefícios deste. Evitar certo evento ou artefato pela probabilidade de erros com potencial catastrófico, como usinas nucleares ou bombas atômicas, pode ser uma exceção por serem claramente perigosos. Em terceiro, as restrições à inovação devem ser o último recurso e não o primeiro como dita o “*by design*”, porque deve ela ser inocente até que se prove o contrário. Especialmente devido à tamanha subjetividade da concordância ou não com certa supressão técnica e, mais importante ainda, como pode-se supor que dará errado um evento que ainda nem aconteceu sem respaldo em experiências anteriores? Quarto, deve-se basear em evidências de possíveis danos concretos e não no medo dos piores casos hipotéticos, porque não só considerar a possibilidade, mas também sempre organizar-se para o pior caso hipotético é altamente penoso, moroso e custoso. Até um copo pode ser uma arma mortal ou qualquer aparelho tecnológico pode ser meio de danos. Quinto e finalmente, onde as intervenções políticas são consideradas necessárias, soluções flexíveis “de baixo para cima”, de natureza responsiva, são quase sempre preferíveis a controles rígidos e “de cima para baixo”, de natureza antecipatória. Aliás, esta é lógica base

de todo o liberalismo. É complicado notar as consequências que designs de artefatos podem gerar na humanidade como um todo e não é fácil visualizar como poderíamos ser sem os mesmos. Só quando algo é realmente maléfico em alguma instância, nos perguntamos a necessidade daquilo e se é evitável. Sendo válido o argumento que sustenta o *by design* de que, muitas vezes, não é fornecida outra solução a não ser sugerir uma volta ao estado anterior à inexistência daquele artefato e isto raramente é possível, portanto, a precaução seria justificável.

Os defensores do princípio da precaução como posição geral padrão acreditam que inovações devem ser reduzidas ou proibidas até seus desenvolvedores provarem que não causarão danos a indivíduos, grupos, entidades específicas, normas culturais ou jurídicas. É sempre difícil, todavia, encontrar uma forma de avaliar as compensações associadas à precaução. Ao se precaver sobre algo, sempre há a indagação se ele não causasse prejuízos de certa maneira, problema este que enfrentam aplicadores da LGPD no mercado hodierno tão doutrinado a buscar o máximo de lucro e, portanto, de dados pessoais dos clientes. Além disto, há uma dificuldade de se elaborar uma definição do que constitui o dano tecnológico no dinâmico mundo globalizado. No presente trabalho, encontramos sempre uma dificuldade em descobrir o custo-benefício de certa restrição, mas analisamos cada problema especificamente.

Observemos que o futuro da política tecnológica emergente tende e tenderá à: arbitragem da inovação, em que inovadores regularmente mudam-se para jurisdições que forneçam um ambiente legal menos regulatório, como no caso de globais provedores da internet que tem seus servidores em países com maiores flexibilidades legislativas; desobediência civil tecnológica, que representa a recusa de consumidores em obedecer a regulamentos que consideram ofensivos, confusos e/ou demorados, como no caso de pirataria de livros e artigos científicos – como o *Sci-Hub* – ou de produções cinematográficas – através do download por torrentes; e desregulamentação privada espontânea, pela eliminação dos regulamentos tradicionais devido a uma combinação de rápidas mudanças tecnológicas. Apesar de termos visto que, na História, há a presença incessante da técnica dominadora e inibidora do humano do homem, ele geralmente não quer estar sempre submisso. É possível notar a tendência global de massas migratórias de países mais totalitários a países mais liberais, ou seja, o ser humano tem o espírito de querer ser mais livre. Para liberais, os remédios legais propostos costumam ser inadequados para resolver problemas de segurança virtual. Eles veem com bons olhos as instituições informais e privadas que aplicam as normas de segurança de rede na internet numa cooperação conjunta. Todavia, como mostramos neste trabalho, as empresas não são suficientemente eficientes na quase-anárquica rede. Pelo contrário, há múltiplos problemas na falta de uma maior prevenção, coerção e coordenação conjunta. Ressaltamos a possibilidade de

que, hipoteticamente, com mais poder estatal na rede, contextos sociais poderiam piorar, como no caso da Coreia do Norte.

Outro argumento contra a necessidade de se preocupar com a moralidade de uma inovação *by design* é a injustificação do pânico, pois há sempre fortalecimentos de sistemas e educação do público sobre os riscos. Esta injustificação é corroborada pela criatividade humana. É o exemplo da cultura do bom tratamento de dados da LGPD que deve ser adaptada aos ciberconsumidores de apps na rede. Juristas e entes públicos tem a árdua missão de educar os cidadãos a cuidarem de seus próprios dados, para não se inscreverem e utilizarem qualquer aplicativo, provedor ou website da rede, pois um uso desenfreado pode e provavelmente acarretará em danos aos seus direitos. Consumidores, empresas e outras organizações, com o tempo, aprendem a lidar e resistir criativamente diante dessas ameaças. O medo da tecnologia não é novidade, pois sempre houve uma desconfiança histórica. Acreditava-se que telefones, relógios e televisões interromperiam a vida das pessoas, prejudicando a produtividade. E, de certa forma, isto ocorreu, mas a maioria da população considera que os benefícios compensaram os estressores. Para eles, novas tecnologias estão tornando nossas vidas diferentes, mas não necessariamente mais estressantes ou piores do que teriam sido sem elas.

O problema dos sistemas reguladores tradicionais “de cima para baixo” são seus procedimentos serem excessivamente rígidos, burocráticos e lentos para se adaptar às novas realidades. Eles se concentram em remédios preventivos que visam prever o futuro e problemas hipotéticos que talvez nunca ocorram. Pior ainda, a regulamentação administrativa pode impedir experimentos benéficos que produzem novas e melhores maneiras de fazer as coisas, mas sem saber se seria pior não tê-la. Aumentando assim o custo de iniciar um empreendimento comercial e geralmente desestimulando atividades que possam beneficiar a sociedade, especialmente desencorajador para os pequenos negócios, sempre os maiores prejudicados por mais regulamentações. Se as políticas públicas fossem guiadas a todo momento pela mentalidade de precaução, a inovação se tornaria impossível pelo medo do desconhecido e dos cenários hipotéticos de pior caso, superando todas as outras considerações. Em termos práticos, esta precaução significaria menos serviços, produtos de menor qualidade, preços mais altos, menor crescimento econômico e um declínio no padrão de vida geral. Um exemplo das tentativas de combate a um problema técnico são os casos de várias ONGs ou de defensores do meio ambiente que são contra o latifúndio, os agrotóxicos ou a indústria agropecuária, quando estes garantem a grande maioria da alimentação mundial. Devemos, como juristas, buscar auxiliar a sociedade a tornar-se mais igualitária e menos agressiva ao meio ambiente. Técnicas de aprimoramento para menos nocividade de agrotóxicos devem ser alcançadas. Uma forma de

lidar inteligentemente com este problema é a de veganos e de vegetarianos, pois utilizam do discurso de que matar e consumir só plantas é preferível a também comer animais e que causa menos danos ao meio ambiente, o que pode ser bem verdade. Assim, a busca por essa mudança de hábito pode levar a mais sustentabilidade. Estes são exemplos de mudanças de hábitos que sustentam a ideia de que devemos priorizar a mudança da demanda e não só da oferta, pois, no contrário, qualquer solução geralmente não obtém resultados positivos. Parece ser mais razoável verificar como a sociedade reagirá e utilizará certo artefato, para depois tomar alguma decisão. Assim, a lógica é sim pautada na prevenção, mas na prevenção fruto da experiência de certa tecnologia no mercado e não na percepção de algum futuro imaginário. A experiência deve ditar a prevenção.

Artefatos, tecnologias e tudo aquilo que encontramos na internet possui algum aspecto preventivo em seu design, seja pelo aprendizado por experiências anteriores ou por pura abstração de um possível futuro. Há aqueles também que servem justamente à prevenção. Não é disso que tratamos. A discussão é sobre medidas que podem limitar completamente o desenvolvimento da internet, de empresas e de nós usuários ou moldá-la às morais e diretrizes aleatórias de algum ente estatal restritivo e antidemocrático. Certamente, devem todos atributos da internet ser o menos maléfico possível ao ciberusuário. Empresas e Estados devem buscar o estoque mínimo de dados e imagens – com o reconhecimento facial em alta – dos usuários, pela prevenção *by design* a possíveis *data breaches*, invasões hackers e mal uso por seus funcionários públicos e privados. Mas prevenir o desenvolvimento de tecnologias, quando não se sabe suas consequências, parece não ser o mais indicado.

Na toada jurídica, quando um ordenamento decreta uma sanção ou dever, busca mitigar certa ação danosa, ou seja, almeja a precaução de que certo comportamento não aconteça. Neste sentido, são justos os deveres e direitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Regulamentos, como o Digital Services Act, melhoram a moderação democrática – sempre respeitando a presunção da inocência e o devido processo legal – de conteúdo em plataformas de mídia social sobre conteúdo ilegal. Estas normas regulamentadoras do comportamento na rede responsabilizam usuários sobre seus atos ilícitos e intermediários-provedores sobre o conteúdo alheio não-moderado – quando sabem que é ilegal e não o removem –, prevenindo a recorrente supressão do direito dos ciberusuários de serem autodeterminados pelo que permitem.

### 3.5.2 Direito de Fazer Nada

*Tudo aquilo que não prejudica a natureza ou o ser humano é um luxo para quem pode e não para quem quer.*

No subcapítulo “História do Homem Técnico”, vimos que havia técnica desde as primeiras atividades do homem primitivo e quando um ser humano resigna “em nome da consciência” – porque o uso de certa técnica ou tecnologia pode lhe fazer mal – e não faz o que lhe é pedido ou socialmente imposto, é condenado por não ser cidadão responsável, é um desempregado, vagabundo, ignorante ou inútil pois não consegue modificar eficientemente toda a sociedade. Ao abster-se, ele se condena a uma série de restrições que influenciam diretamente seus direitos. A obediência à coordenação social é produzida artificialmente pelo próprio homem e ele se autossabota em crer, sem se indagar, que tais técnicas são para um bem comum, porque a injustiça é preferível à descoordenação social. A imposição técnica dá sentido à vida de muitos.

Vimos também que a eficácia de uma determinada técnica é medida a partir da sua capacidade de ser aplicada ao homem sem gerar protestos, como no perigoso e automático reconhecimento dos benefícios da colheita de informações pessoais por *cookies* para uma experiência diferenciada. A inevitabilidade do progresso técnico gera a desresponsabilização, já que o homem seria uma mera vítima do mundo, como se não tivéssemos controle mais do que somos ou fazemos e, assim, a técnica nos afasta de nossa mentalidade. Mas devemos nos responsabilizar e tomar alguma atitude sobre aquilo que nos afeta e consideramos ser maléfico.

Afastar-se de alguma tecnologia ou da internet pode ser fruto de um analfabetismo tecnológico, ou seja, de uma incapacidade em mexer com a tecnologia moderna, levando à exclusão digital, uma forma mais moderna de violência e ampliação de desigualdades. Mas há outro contexto, o do afastamento intencional.

Quem escolhe conscientemente ficar fora da internet, mesmo sendo prejudicado e invisibilizado, escolhe sofrer as consequências do não uso. Às vezes, esta desintoxicação digital é para evitar ou controlar o vício biológico, como vimos anteriormente, quando não é para resolver problemas de sono, sintomas depressivos, desregulação no humor e aumento dos níveis de estresse. Seja por desconhecimento do uso, seja por escolha consciente, o não uso de tecnologias limita drasticamente até direitos básicos como alimentação (são cada vez mais raros os restaurantes que não usam o cardápio 100% digital através de um QR Code), finanças (não é possível mais usar um banco sem e-banking), compras (a internet nos faz trabalhar até na

função de vendedor e caixa de supermercados e lojas). Mas não se enganem, quando empresas nos dão indicações de como usar um aplicativo, estão terceirizando algum serviço a nós consumidores. Se acha que algum serviço ou aplicativo é de graça, é porque você é o produto.

Como visto no subcapítulo “Consentimento Quase-Tácito”, a possibilidade de recusa é possível, mas são raros os usuários que deixam de utilizar uma rede, provedor ou aplicativo por discordância aos seus termos, por exemplo por falta de opções. Quem dirá desligar-se completamente da internet. Aqueles que optam pela exclusão total, sofrem diversas consequências. Se o indivíduo escolhe não utilizar as redes sociais mais populares, se isolará quase completamente, pois a maioria permanecerá nelas. Há maior variedade aplicativos e websites de comunicação, mesmo assim é complicado abandoná-las.

Ninguém precisa estar na rede, é possível (sobre)viver sem se comunicar com ninguém até pessoalmente, quem dirá virtualmente. Mas, nesta Era Digital, a busca pelo equilíbrio entre a vida pessoal e o trabalho pode também ser difícil. O usuário que quer permanecer conversando com seus amigos, interagir como qualquer ser humano, não tem a real opção de sair. O usuário que precisa dessas plataformas para interagir com colegas até dentro do trabalho, ou para se exporem para fins de empregos, também não têm muito para onde fugir.

Cada vez mais que nos inserimos na Era Digital e nas tecnologias, cada vez mais fica difícil assimilar uma forma de vida que seja impossível de ser assimilada pela lógica da técnica. A noção de ética do não-poder de Ellul contrasta com a atual ideia da internet como um Destino Manifesto americano e não como uma ferramenta de convivencialidade e troca de experiências.

Afastar-se da internet e de algumas tecnologias é uma decisão ética e moral. E o grande problema da moralidade e das soluções éticas é quando perpassa uma justa escolha pessoal e busca a aceitação e obediência das outras pessoas a ela, como na propaganda da desintoxicação tecnológica. Uma das soluções que trazem é a ideia de uma internet mais localizada, como um *open source* que só permite comunicar com quem está perto. Mas provavelmente essa é uma solução utópica porque escapa nossa realidade pensar em ativamente nos limitar, neste caso a comunicação, sem absolutamente nenhum malefício evidente, como maiores custos monetários. Por que não poder conversar com alguém de outro estado ou país se podemos, através de um aplicativo? Esta ética do não-poder, que busca contradizer a lógica técnica e controlada, seria de difícil aplicação real.

No mundo capitalista, resistir à economia de produção com o “fazer nada” também parece ser uma difícil tarefa. Seres humanos subsistem através do trabalho a milênios. Presumemos que um indivíduo se sustenta através de uma atividade laboral que não necessita tanto de tecnologias ou tem uma vida complementemente autossustentável. Exceto para sobreviver e

sustentar aqueles que é responsável, como filhos, tem ele o direito de nada fazer. Mas dificilmente alguém hoje pode ser autossustentável. Quando envolvemos as interações e responsabilidades sociais na equação, torna-se ainda mais difícil. Diferente da vida pessoal, não é possível o exercício do direito de fazer nada quanto ao trabalho.

No Direito Trabalhista, temos o Direito à Desconexão. Com a adoção em larga escala do teletrabalho, especialmente durante a pandemia da COVID-19, os limites entre a vida profissional e a pessoal se misturaram para muitos trabalhadores. Diante disso, a comunidade jurídica discutiu o direito à desconexão, ou seja, o direito do trabalhador de poder aproveitar o tempo fora de sua jornada de trabalho para atividades pessoais – de lazer ou familiar – que não esteja relacionada à atividade profissional. Em princípio, não há previsão legal expressa no Brasil sobre o direito à desconexão. Nos últimos anos, a expressão aparece cada vez mais em demandas judiciais, especialmente quanto a jornadas de trabalho que comprometem o descanso e o convívio social e familiar e ao empregador não poder exigir comunicação, por qualquer meio de comunicação eletrônica, fora do horário de trabalho. Existe também Projetos de Lei que tratam desse desempenho laboral fora da jornada a ser contada como hora extra. Este direito à desconexão assegura o respeito ao período de descanso e à intimidade pessoal e familiar para evitar prejuízos à saúde mental dos funcionários.

Além do escopo trabalhista, é possível diminuir o uso de técnicas e tecnologias em geral. A literatura dá exemplos como a jardinagem que não busca eficiência máxima. Todavia, hoje um restaurante com alimentos sem agrotóxicos é só para quem pode, tornando-se quase *gourmet*. Alimentos naturais são mais escassos e mais caros. Aliás, a moral hodierna é a de que tudo aquilo que não prejudica a natureza ou o ser humano é um luxo para quem pode e não para quem quer.

A discussão de não fazer nada questiona até que ponto é da natureza humana as técnicas. Ao “fazermos nada” estaríamos no rumo de sermos “mais humanos”, inclusive com o outro? A experiência humana é o contexto sensitivo pelo experimento com o meio, outros humanos inclusos. Se o homem primitivo passava menos tempo com sua lança, pedra lascada ou pele de animal em seu corpo, ele estava experimentando a natureza e outros seres mesmo assim. Natureza, outros humanos ou artefatos artificiais – naturezas modificadas – são fontes de experiências que vão se aprimorando com o tempo. É da natureza humana, animal ou até de seres vivos como plantas querer ser o mais eficaz possível e por isso o somos. Ser animal é, além de instintivo e emotivo, ser essencialmente um sobrevivente eficaz. E ser racional é uma tradução mais elaborada do nosso instinto de sobrevivência eficaz e, após consciência, de viver feliz e harmonicamente. Ser racional parece ser tecnicamente eficiente. Não houve momento

histórico em que o homem deixou de (querer) ser eficiente ou interagir tecnicamente com seu meio.

O direito de fazer nada é possível, mas essa liberdade que se ganha (em forma de tempo não consumido por técnicas) seria para ser e ter o que? Sem técnicas, como em limitações na internet e em tecnologias, seríamos mais humanos para conosco e com o próximo? Parecem os meios serem importantes para, inclusive, o indivíduo buscar ser e ter o que bem quiser e é a técnica ou o seu “querer ser eficiente” que disponibilizam estes meios.

Enfim, o exercício do direito de fazer nada reflete sobre nossa capacidade de ignorar a realidade quando é doloroso demais reconhecê-la e modificá-la, quando nos submetemos a técnicas e falácias de que nada podemos fazer a respeito. Apesar de custosa, é possível tomar uma posição ativa de abstenção contra técnicas que consideramos maléficas. Quando vários indivíduos ignoram a dureza da realidade, submetendo-se inquestionavelmente às técnicas, gera-se uma cultura de aceitação e de autossabotagem que legitimam e normalizam abusos de direitos pela técnica e isto não pode acontecer.

### 3.5.3 Sabotar a Técnica

*Os homens podem ser classificados como cegos-surdos-mudos bem-intencionados.*

Para Jacques Ellul (1968), não há mais como nos livrarmos completamente da eficácia da técnica, trata-se de uma batalha perdida, já que nossas ações têm sempre alguma técnica seguida inconscientemente a qual somos seus meros instrumentos. Mas o presente autor desta dissertação vislumbra o livramento de técnicas especificamente piores, mesmo que seja pela substituição por outra técnica a solução. Por exemplo, o ideal social é utilizar carros particulares para o trabalho a fim de chegar mais rápido e, logo, haver menor perda de tempo e tê-lo mais para o lazer e mais trabalho. Se um indivíduo toma a decisão de ir trabalhar através de transporte público ou de bicicleta, tão somente para poupar o meio ambiente, com o malefício de triplicar seu tempo de locomoção, ele estaria se livrando e substituindo esta técnica a outra melhor, em uma retirada consciente da eficácia. Neste raciocínio, se segue o presente capítulo. São vários os exemplos de técnicas benéficas do Estado, principalmente para aqueles com democracias mais consolidadas e de maiores Índices de Desenvolvimento Humano (IDHs). Muitos destes países somente alcançaram este status com medidas de sabotagem. No Brasil, a maioria das

ações estatais e jurídicas não encontraram ainda seu ideal provimento à boa vida. Todavia, bons exemplos existem sobre qualquer espectro social, frutos do Estado ou do particular, e devem ser perquiridos a despeito das dificuldades.

A identificação da eficácia e da técnica no comportamento humano já preocupava estudiosos desde muito tempo. Em 1921, Thorstein Veblen (2001, p. 4) sugeriu uma forma de negar ou de, pelo menos, amenizar os malefícios da técnica. Essa forma foi denominada pelo mesmo de sabotagem. Para ele, o significado comum da palavra sabotagem é a “retirada consciente da eficiência”. Mas toda essa estratégia de atraso, restrição, impedimento e derrota perante a técnica é do mesmo caráter da sabotagem capitalista ou até sindicalista que trabalhadores no século XX falavam. Derrota porque o indivíduo, ao não agir mais de forma eficaz, estará perdendo todos os benefícios e confortos desta submissão e, ainda mais, estaria contra um sistema de pessoas e mecanismos jurídicos-sociais que estão inteiramente entregues à técnica e à vontade eficaz, trazendo vários prejuízos ao mesmo com isto, em detrimento de ser mínima e temporariamente “livre” da técnica específica que se libertou. Assim, usamos corretamente a palavra ao aplicá-la como um recurso à restrição pacífica, um atraso, retirada ou obstrução (VEBLEN, 2001, p. 4). Note-se que a sabotagem geralmente funciona dentro da lei e, por isso, não se trata de uma revolução contra o capitalismo ou um golpe de estado, embora muitas vezes possa estar dentro da moral e não no espírito da lei. É uma escolha pessoal (VEBLEN, 2001, p. 6) e, no caso de um Estado ou de uma instituição financeira ou empresarial, uma retirada ou mudança voluntária de suas forças.

Ao contrário do senso comum, são diversas as medidas de política e gestão, tanto nos negócios privados quanto na administração pública, que são inconfundivelmente de natureza da sabotagem e que não são apenas consideradas boas, mas deliberadamente sancionadas pelo direito comum ou privado e pela consciência pública. Muitas dessas medidas são essenciais e acredita-se fielmente que são indispensáveis ao bem comum (VEBLEN, 2001, p. 7), como a restrição de produção para manter os preços em um nível razoavelmente lucrativo e, assim, evitar depressão nos negócios; ou quando a Louis Vuitton queima estoque morto favorecendo a balança de oferta-demanda, onde acreditam ser o mais benéfico; ou o direito à greve, situação tão anti-eficaz para a produção; ou a escolha de um indivíduo em abrir mão de ganhar mais dinheiro em prol de menos tempo de trabalho, dentre outros exemplos possíveis.

Os meios desse controle necessário de produção da indústria são necessariamente algo na natureza da sabotagem – no modo de retardo, restrição, retirada, desemprego de trabalhadores – pelo qual a produção é mantida aquém de sua capacidade (VEBLEN, 2001, p. 8). A indústria mecânica é excessivamente produtiva. Portanto, a taxa e o volume da produção

precisam ser regulados com vistas ao que o tráfego suportará, ou seja, o que trará o maior retorno líquido em termos de preço. Caso contrário, haveria uma superprodução, depressão nos negócios e consequentes tempos difíceis ao mercado. Superprodução significa produção que excede o que o mercado realizará a um preço suficientemente lucrativo. Assim, a prosperidade de um país ou empresa, muitas vezes, depende de uma “retirada consciente de eficiência” pelos homens de negócios que controlam a produção industrial e os Estados (VEBLEN, 2001, p. 11), mas, muitas vezes, não por alguma ética e sim pelo lucro final. Nota-se, porém, que nem toda retirada é sinônimo de algo benéfico. A título de exemplo, a citada queima de estoque morto da Louis Vuitton pode até ser benéfica à empresa por manter seus altos preços, sua continuidade e benefícios ao mercado (como a empregabilidade e sustento de famílias), porém é plenamente questionável ao bem comum, já que estes produtos poderiam ser doados a quem precisa. Diversos restaurantes e supermercados jogam fora alimentos que poderiam ser consumidos por aqueles que passam necessidade. Apesar de guerras serem, muitas vezes, jogadas financeiras de certos empresários, um país, ao ser atacado e precisando se defender por exemplo, precisa retirar conscientemente investimentos na educação e saúde e pô-los em indústrias bélicas e exércitos. Independente das consequências, a presença da sabotagem é notória. Compreendemos a prática empresarial, mas não é surreal pensarmos em medicamentos (em farmácias) ou alimentos (de restaurantes como citamos) sendo jogados fora com tantas pessoas passando necessidade dos mesmos.

Um lucro razoável sempre significa o maior lucro possível. Se os empresários responsáveis, por alguma aberração casual, se afastarem desse caminho reto e estreito de integridade comercial e permitirem que as necessidades da comunidade influenciem indevidamente em seu gerenciamento industrial, na maioria dos casos, eles se sentiriam desacreditados e provavelmente enfrentariam insolvência. Nem a própria sociedade, o próprio povo, acreditaria em suas boas intenções. Observe-se que nesse caso sua única salvação é uma retirada consciente da eficiência. Ou seja, como o ditame da técnica na sociedade hodierna é a busca incessante pelo lucro máximo, na maioria dos casos, a vontade de não buscá-lo é uma retirada consciente da técnica. Todavia, por exemplo, hoje há críticas sociais a certas empresas que utilizam de bandeiras verdes de defesa ao meio ambiente ou de defesa de igualdade de gênero ou de defesa dos direitos dos LGBTQI+ (*Lesbian, Gay, Bisexual, Transgender, Queer, & Intersex Life*) somente para atração do público jovem, sendo quase visível que não se preocupam tanto na prática com estes direitos, com políticas e atitudes internas contraditórias a essas propagandas. É difícil vislumbrar uma ação empresarial que não visa exclusivamente o lucro. São diversos os casos de espécies “empresas comunitárias” que buscam, por exemplo, a

distribuição igualitária do lucro entre os funcionários, mas escassas aquelas que dão certo. Se a moral de certo país é de proteger o meio ambiente a qualquer custo e uma empresa escolhe tomar as piores decisões possíveis quanto ao equilíbrio da natureza, ela está igualmente se retirando conscientemente da técnica específica daquele país de defesa à sua flora e fauna *v.g.* Portanto, esta retirada ocorre quando o ente age em desconformidade com a técnica que lhe é imposta; se ela será benéfica ou não, cabe uma análise específica. Já a grande ilustração de sabotagem administrada pelo governo é a tarifa protetora. Protege certos interesses especiais, obstruindo a concorrência além da fronteira (VEBLEN, 2001, p. 13-15). A matemática do custo-benefício é clara, de que a manutenção de empresas locais vale mais a pena para o próprio povo do que pagar por aquele mesmo produto mais barato, tratando-se aqui de sabotagem pois é diretamente antilucrativa para a sociedade. Indiretamente, a discussão é milenar principalmente no que tange às empresas empregarem cidadãos no próprio país e os impostos pagos por elas e por estes empregados gerariam mais renda para maiores investimentos públicos e, portanto, mais benefícios a mesma. Liberais questionam esta conta pelos maus investimentos públicos.

Não temos a intenção de encontrar falhas nos usos da sabotagem. Não é uma questão de moral e de boas intenções. Deve-se presumir sempre que, mesmo em tempos difíceis como a presença de corrupções sistêmicas, o espírito orientador em todas essas ações governamentais e empresariais para regularizar os assuntos da nação, seja por restrição ou por incitação, é uma solicitude sábia pelos ganhos e segurança da nação, somando-se todas pessoas físicas e jurídicas (VEBLEN, 2001, p. 16).

Deste 1921, observava Veblen que o avanço progressivo desse sistema industrial em direção a um equilíbrio mecânico parece estar se aproximando de um passo crítico, além do qual não será mais possível deixar seu controle nas mãos de homens de negócios que trabalham com objetivos diferentes para fins particulares (VEBLEN, 2001, p. 37). O avanço contínuo da tecnologia mecânica exigiu um volume e uma diversidade cada vez maiores de conhecimentos especiais e assim deixou os empresários continuamente cada vez menos capazes de compreender o que é exigido de equipamentos e pessoal industrial, isto é, alienaram-se. Isso foi antes da indústria mecânica ter ido longe em escopo, complexidade e especialização o qual fora crítica de Marx (1867), antes também do trabalho contínuo dos tecnólogos levar o sistema industrial a uma capacidade produtiva tão alta que corria o risco de produzir um produto maior do que o necessário para um negócio lucrativo (VEBLEN, 2001, p. 39).

Esses especialistas, tecnólogos ou engenheiros formam o Estado-Maior indispensável do sistema industrial. Sem sua orientação e correção imediatas e constantes, o sistema industrial

não funciona. Eles são um cruzamento entre um especialista em tecnologia e um agente comercial, cercado pelas limitações de ambos e não é totalmente competente em nenhuma das linhas (VEBLEN, 2001, p. 44-45).

Nossa geração se perguntaria por que deveríamos nos preocupar. O que poderíamos ganhar? Foi o que nossos antepassados se perguntaram, continuamente despreocupados com a degradação ambiental por exemplo. E a geração mais jovem, se não for tão interessada pela experiência comercial, terá a mesma probabilidade de se perguntar o que temos a perder. O presente trabalho trata, não só de grandes, mas de quando fazemos pequenas abstinências e submissões inconscientes gerando desconhecimento de nosso pretexto, alienando-nos sobre o mundo e acarretando em nosso adestramento perante à técnica, eficácia e tecnologia.

Para os fins dessa nova ordem de produção projetada, portanto, os homens podem ser classificados como homens cegos-surdos-mudos bem-intencionados, uma definição de um técnico ou engenheiro. Seu julgamento mais sábio e seus esforços mais sinceros se tornam sem sentido e equivocados – demasiado sensíveis – tão logo o objetivo de controle da indústria muda da base de lucros dos investimentos ausentes para a de uma produção útil de bens (VEBLEN, 2001, p. 91). E, hodiernamente, o homem cego-surdo-mudo bem-intencionado vem ganhando outra faceta, o de máquina.

Os técnicos não têm o hábito de ter uma visão muito diferente de seu próprio caso. Assim sendo, eles ainda sentem que, na natureza das coisas, se encaixam como empregados daqueles homens de negócios empreendedores que são, na natureza das coisas, eleitos para receber algo por nada (VEBLEN, 2001, p. 93). A atual aparência do mundo é de que todos seres humanos são coitados de sua experiência, de suas faculdades físico-químicas e da sociedade e do meio. Não havendo culpa, não há o que mudar. Somos todos vítimas do jeito que o mundo é desde quando chegamos ao mundo. E, assim, a técnica e a tecnologia mudam este mundo e acabam nos modificando sem oposição. Se não assumirmos nossa culpa como seres que colocam a eficácia em primeiro lugar, não há como parar a técnica quando destrutiva. Daí a importância da sabotagem, retirada consciente da técnica, para podermos, ao menos, escolher a qual outra espécie de técnica, preferencialmente uma mais humana, nos submeteremos.

Já tomamos decisões pela única razão de felicidade, em detrimento de mais dinheiro ou que tiveram custos. Todos seres humanos já escolheram momentos de paz em detrimento de confortos fáceis, banais ou passageiros. Não é preciso ser um super-homem nietzschiano (*übermensch*) (NIETZSCHE, 2002), superando a humanidade “incapacitada pela gloriosa técnica”, para se desvencilhar parcialmente, tendo que deixar a felicidade – quando padronizada e banalizada pela normalidade e supremacia das massas, como o ser feliz é ser assim ou ter

aquilo – de lado por ser suposto impedimento ao bom senso. Ellul doutrina como a técnica está impregnada no ser humano e na sociedade e, de fato, não é possível nos desvencilharmos completamente da “vontade de ser eficaz”, mas devemos ter atenção especial aos momentos mais íntimos e pessoais. É possível tomar decisões que não se baseiem somente na eficácia absoluta e mensurada por resultados. Ellul e os filósofos da tecnologia querem não só apontar estas tendências desumanizadoras e nos desencenar. Querem, desde já, alertar e, mais que tudo, estimular um comportamento mais humano para conosco e com a natureza. Querem que tomemos mais decisões humanas, que não são impossíveis – tanto que as tomamos, apesar de cada vez menos – pautadas em nossos sentimentos e em defesa de nossa liberdade e dignidade, a fim de que não vendamos por pouco nossa liberdade de autodeterminarmo-nos.

Nossa liberdade é ameaçada quando a influência que exercemos sobre nossos meios é ofuscada pela influência que esses mesmos meios exercem sobre nós e, por isso, devemos tomar alguma decisão quanto a esta influência desenfreada. O Direito e o Estado devem enxergar o indivíduo não dentro de uma racionalidade técnica de ações mecanizadas. Queremos tratamentos igualitários que façam as pessoas sentirem-se humanas, como um tratamento médico menos desumano ou uma educação mais justa que traga todos pontos de vistas sobre um fato da melhor forma possível. Um bom tratamento público pode levar à dignidade e integridade da vida das pessoas, ao invés de um Estado que só diz ter bons números, mas que a população não sinta diferença em sua tutela. Que pelo menos o Estado permita que essas pessoas tenham a possibilidade de fazerem suas vidas melhores por elas mesmas. Que o Estado não atrapalhe, mas some na vida da maioria. É o que se sugere aqui. Tudo isto através de um Direito menos burocrático e sem sentido de justiça.

## CONSIDERAÇÕES FINAIS

Jacques Ellul foi o primeiro que reconheceu na técnica fundamento para a tecnologia, a maneira dominante e única de responder a todas questões do conhecimento humano, com graves consequências sociais e culturais. O processo técnico transforma seres humanos e a natureza em algo inanimado, morto, técnico, manipulável, previsível e inespontâneo. O racional cessa as possibilidades de erro e, sem escolher para errar, o homem se angustiará menos. A técnica, assim, evita choques e dramas e anestesia o homem para aderi-lo ao inumano. Ao se interessar pelas necessidades imateriais do homem, como sua liberdade e sua autodeterminação, sua principal crítica é o modo como o homem se submete à técnica, com a perda do seu senso social e comunitário, de suas responsabilidades, das autonomias funcionais e sociológicas. Deve o ser humano resgatar seu senso crítico e suas espontaneidades para se autorresponsabilizar e melhorar esta sociedade tão técnica e inumana.

Devemos resgatar nosso senso crítico sobre a sociedade, caso contrário haverá progressivos controles sociais sobre o indivíduo perante os riscos que sempre serão justificativas de mais vigilâncias. Este Estado de progressivos controles, passa a ser um gestor dos riscos, de quem se cobra tão somente que seja eficaz, justificando-se até os constantes Estados de Exceção. Não pode o fim social justificar todos os meios de controle e de retirada da liberdade individual. A ausência de questionamentos dessas tendências impacta seriamente na tutela estatal da internet e qualquer comportamento técnico pode se autojustificar pelo medo do risco e do sofrimento.

No cenário global e no Brasil, há leis que incidem sobre ilicitudes na rede como o Marco Civil da Internet e a Lei de Proteção de Dados Pessoais, mas são pouquíssimas as políticas públicas de combate às mesmas. Direitos são tutelados, mas não são assegurados. Diante das seis características jurídicas do meio digital, é necessário que o Direito Digital tenha uma conotação intervencionista e de direito regulatório. O Direito deve contornar a tendência empresarial de extração do máximo possível de dados pessoais. Quando quase todo aplicativo e *website* contém um Contrato de Adesão genérico e quase todo usuário o aceitando sem ler, a tutela na pertinência do armazenamento deve ser amplamente questionada, pois as empresas e Estados abusam da margem subjetiva do que seria esta pertinência. E não pode o Direito e o povo deixá-los tratar e utilizar seus dados sem nenhum limite palpável. Devemos buscar a cultura de extração e armazenamento mínimo de dados pessoais perante o consentimento quase-tácito. Já a interpretação de cibercrime como crime permanente deverá incidir caso a caso. Afinal, toda vez que o Estado deixa de dar uma resposta célere, fere o direito fundamental dos

indivíduos porque diminui o acesso à segurança do usuário e mal administra recursos pela ineficácia investigativa. Quanto à propriedade intelectual, indagamos o leitor: ao patentear e demorar 15 anos para obter uma licença e ao ter uma polícia que demora anos para solucionar um cibercrime que tenha sido vítima, existe realmente segurança jurídica?

A necessidade desta restrição publicitária mostra-se de mister importância para que uma criança não seja exposta a apelos mercadológicos. Não podem os provedores fazerem uso das informações de crianças e adolescentes para a propaganda personalizada. O Brasil deve se assegurar de que utiliza as melhores ferramentas jurídicas de respeito aos princípios básicos constitucionais para limitar liberdades individuais. No âmbito consumerista, o foro do lugar do consumidor lesado deve ser a regra, com seu domicílio sendo seu centro de interesses. E para solucionar os problemas da rede, a prevenção by design deve se pautar na experiência, pois devem todos atributos da internet ser o menos maléfico possível ao ciberusuário ao mesmo tempo que não devem limitar completamente o desenvolvimento da internet, de empresas e de nós usuários ou moldá-la às morais e diretrizes aleatórias de algum ente estatal. Governanças indiretas, como a ISSO, nascem da necessidade da carência global de tutela dos problemas transfronteiriços.

É gritante a necessidade de reconhecimento nesta sociedade de massas. O indivíduo quer construir uma autoimagem positiva a fim de ser notado. A sensação de pertencimento proporcionada pelas redes sociais ou pela adesão a uma determinada cultura imposta é superficial e ilusória, podendo gerar a perda da identidade, tornando os indivíduos ainda mais vulneráveis aos ataques psicológicos da publicidade. Não devemos sacralizar e adorar sem questionar. Tal moral é hoje tão deturpada que admirar alguém que não tenha coesão de discurso gera uma imagem tal que vale a pena ser ignorante. A técnica e a tecnologia parecem nos fazer agir com reflexo e não refletir sobre algo. Nota-se que a negação da realidade é uma tendência histórica. O ser humano prefere negar a sua realidade e os fatos científicos para a manutenção da sua imagem daquele que sabe mais do que outros, afinal, se reconhecer seu erro ou ignorância, terá sua imagem e sua moral denigradas e isto é inaceitável. Quanto ao nosso futuro, estaríamos na iminência do surgimento do pós-humano? É possível o homem ser ou tornar-se algo que não é humano? O futuro da humanidade deve permanecer cada vez mais incerto, menos determinável e, portanto, mais imprevisível.

A massificação do homem o faz perder grande parte de sua individualidade em meio à sociedade técnica. Na domesticação do homem, ele é obrigado a ser eficaz, caso contrário sofrerá as devidas punições morais e sociais. A constante submissão inquestionável até dos aspectos ruins que sofre dos entraves técnicos que subjagam o seu próprio criador é um perigo.

Devemos questionar nossa atual posição perante o mundo técnico. É assustadora nossa constante autossabotagem ao normalizar algo porque não entendemos ou não podemos pará-lo. Nossa maior preocupação é nossa capacidade de ignorar a realidade quando é doloroso demais reconhecê-la e ainda mais modificá-la.

Todos nós já tomamos decisões, pela única razão de felicidade, que foram em detrimento de receber mais dinheiro ou que até tiveram custos. Todos os seres humanos já escolheram seus momentos de paz em detrimento de confortos fáceis, banais ou passageiros. Não é preciso ser um super-homem nietzschiano para se desvencilhar parcialmente de técnicas. Ellul e os filósofos da tecnologia querem estimular um comportamento mais humano para conosco e com a natureza e objetos. Querem que tomemos mais decisões pautadas em nossos sentimentos e em defesa da nossa liberdade e dignidade, não nos vendendo por pouco. Afinal, não há espaço para sermos, mas sim para simularmos quem somos automaticamente. Temos de mudar esta tendência inumana. Que atentemo-nos e tomemos consciência da imensa influência e poder da técnica e da tecnologia, neste caso da internet, em nossas vidas, evitando decisões humanamente precipitadas e arrogantemente inocentes. Que tentemos sabotar a técnica do nosso dia a dia, uma batalha por vez. Que forneçamos ao homem um tratamento mais humano e justo. E que nos atentemos mais às aceitações tácitas de nossa realidade e da deturpação de nossos direitos, especialmente considerando o dano que gera na nossa psique. Que questionemos tudo possível, especialmente a influência do exterior em nós, a fim de não sermos instrumentalizados por alguém ou algo como a técnica. Quando vários indivíduos ignoram a dureza da realidade, geram uma cultura coletiva de aceitação e de autossabotagem que legitimam e normalizam abusos de direitos e isto não pode acontecer.

O Direito tem que estar de acordo com a justiça de seus cidadãos no caso da internet. Deve o Estado enxergar o indivíduo não dentro de uma racionalidade técnica, cujas ações tem que ser necessariamente mecanizadas e automáticas. Que o Estado permita que pessoas façam suas vidas melhores por elas mesmas na rede; que não atrapalhe, mas some na vida da maioria. É o que se sugere aqui.

## REFERÊNCIAS

ALBERTIN, Luiz Alberto. **Comércio Eletrônico**: modelo, aspectos e contribuições de sua aplicação. 5. ed. São Paulo: Atlas, 2004.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução: Viroílio Afonso da Silva. São Paulo: Malheiros, 2009. Título original: Theorie der Grundrechte.

ALVES, Felipe Otávio Moraes. **A Tutela do Estado sobre Cibercrimes de Hackers**. Goiânia: Espaço Acadêmico, 2019a.

ALVES, Felipe Otávio Moraes. Cibercrime como Crime Permanente. *In: THE ELEVENTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE AND CYBER LAW*, 11. ed., 2019, São Paulo. **ICOFCS 2019**. São Paulo: ICOFCS, 2019b. p. 29-42. DOI 10.5769/C2019004.

ARANHA, Márcio Iorio. **Manual de Direito Regulatório**: Fundamentos de Direito Regulatório. 2. ed. Coleford: Laccademia Publishing, 2014.

ATENDIMENTO Automatizado ao Cliente. *In: Love, Death + Robots*. Criação: Tim Miller, David Fincher, Jennifer Miller e Joshua Donen. Roteiristas: John Scalzi, Meat Dept (Kevin Van Der Meiren, David Nicolas, Laurent Nicolas) e Tim Miller. Direção: Jennifer Yuh Nelson e Meat Dept. Estúdio de animação: Atoll Studio. Realização, Distribuição e Produção: Netflix. Los Gatos: Netflix Streaming Services, 14 maio 2021. Primeiro episódio do Volume II da série. 12min, son., color. Acesso em: 4 fev. 2022.

BARROSO, Luís Roberto. Liberdade de expressão versus direitos da personalidade: Colisão de direitos fundamentais e critérios de ponderação. *In: SARLET*, Ingo Wolfgang (org.). **Direitos fundamentais, Informática e Comunicação**. Porto Alegre: Livraria do Advogado, 2007.

BBC NEWS. Is your phone listening in? Your stories. **BBC News**, London, 30 Oct. 2017. Tech. Disponível em: <https://www.bbc.com/news/technology-41802282>. Acesso em: 10 fev. 2022.

BERETTA, Pedro. Sem meios eficazes, Lei Carolina Dieckmann até atrapalha. **Revista Consultor Jurídico**, São Paulo, 10 maio 2014. Direito Penal. Disponível em: <https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha>. Acesso em: 10 fev. 2022.

BESTUZCHEV, Dmitry. 12 ataques de malware por segundo. *In: 6ª CONFERÊNCIA LATINO-AMERICANA DE ANALISTAS DE SEGURANÇA DA KASPERSKY*, 6. ed., 30 ago. 2016, Los Cabos. **Kaspersky Daily**. São Paulo: Kaspersky, 2016. Disponível em: <https://www.kaspersky.com.br/blog/internautas-sofrem-12-ataques-de-malware-por-segundo-na-al/6500/>. Acesso em: 22 fev. 2022.

BISCHOFF, Paul. 2.7 billion email addresses exposed online, more than 1 billion of them include passwords. **Comparitech**, Maidstone, 10 Dec. 2019. Information Security. Disponível em: <https://www.comparitech.com/blog/information-security/2-7-billion-email-addresses-exposed-online/>. Acesso em: 29 jan. 2022.

BISCHOFF, Paul. Report: 250 million Microsoft customer service and support records exposed on the web. **Comparitech**, Maidstone, 22 Jan. 2020a. Information Security. Disponível em: <https://www.comparitech.com/blog/information-security/microsoft-customer-service-data-leak/>. Acesso em: 29 jan. 2022.

BISCHOFF, Paul. Report: 267 million Facebook users IDs and phone numbers exposed online. **Comparitech**, Maidstone, 09 Mar. 2020b. Information Security. Disponível em: <https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/>. Acesso em: 29 jan. 2022.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. 15. ed. São Paulo: Saraiva, 2010.

BOECHAT, Lucas. Provedores de Internet no Brasil. **Tech in Brazil**, São Paulo, 12 nov. 2015. Internet. Disponível em: <https://techinbrazil.com.br/provedores-de-internet-no-brasil>. Acesso em: 12 fev. 2022.

BONAVIDES, Paulo. **Curso de direito constitucional**. 22. ed. São Paulo: Malheiros, 2008.

BOSTROM, Nick; SANDBERG, Anders. The wisdom of nature: an evolutionary heuristic for human enhancement. In: SAVULESCU, Julian; BOSTROM, Nick (ed.). **Human enhancement**. Oxford: Oxford University Press, 2009.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 22 abr. 2022.

BRASIL. **Convenção sobre o Cibercrime**. Brasília, DF: Ministério Público Federal, 2001. Disponível em: [http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf). Acesso em: 12 fev. 2022.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 22 abr. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2019. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 22 abr. 2022.

BRASIL. Supremo Tribunal de Justiça (1ª Turma). **Recurso Ordinário em Mandado de Segurança n. 15146/SC**. Recurso Ordinário. Ministério Público. Sigilo bancário. Direito relativo. Suspeita de crime financeiro. Recorrente: Waldemiro Hauck. Recorrido: Ministério Público Federal. Rel.: Min. Luiz Fux, Data de Julgamento: 18/03/2003, Data de Publicação: 07/04/2003. Disponível em: [https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num\\_registro=200200876097](https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=200200876097). Acesso em: 22 fev. 2022.

BRASIL. Supremo Tribunal de Justiça (3ª Turma). **Agravo Regimental no Agravo de Instrumento n. 1320633/SP**. Agravo Regimental. Exceção de incompetência. Cláusula de eleição de foro. Validade, desde que ausente a hipossuficiência da parte aderente e inexistente a inviabilização do acesso ao Poder Judiciário. Acórdão recorrido em harmonia com o entendimento desta corte. Existência de abusividade. Onerosidade excessiva. Reconhecimento. Impossibilidade de reexame de provas. Incidência da Súmula 7 desta Corte. Recurso Improvido. Agravante: Luiz Verner Klein e outro. Agravado: BASF S/A. Rel.: Min. Massami Uyeda, Data de Julgamento: 26/10/2010, Data de Publicação: 11/11/2010. Disponível em: [https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num\\_registro=201001043243](https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201001043243). Acesso em: 22 fev. 2022.

BRASIL. Supremo Tribunal de Justiça (4ª Turma). **Recurso Especial n. 63981/SP**. Direito do Consumidor. Filmadora adquirida no exterior. Defeito da mercadoria. Responsabilidade da empresa nacional da mesma marca (“Panasonic”). Economia globalizada. Propaganda. Proteção ao consumidor. Peculiaridades da espécie. Situações a ponderar nos casos concretos. Nulidade do acórdão estadual rejeitada, porque suficientemente fundamentado. Recurso conhecido e provido no mérito, por maioria. Recorrente: Plinio Gustavo Prado Garcia. Recorrido: Panasonic do Brasil LTDA. Rel.: Min. Aldir Passarinho Junior, Data de Julgamento: 11/04/2000, Data de Publicação: 20/11/2000. Disponível em: [https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num\\_registro=199500183498](https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=199500183498). Acesso em: 22 fev. 2022.

BRASIL. Supremo Tribunal de Justiça (4ª Turma). **Recurso Especial n. 844736/DF**. Internet. Envio de mensagens eletrônicas. Spam. Possibilidade de recusa por simples deleção. Dano moral não configurado. Recurso Especial não conhecido. Recorrente: Gérson Alves de Oliveira Júnior. Recorrido: WB Restaurante LTDA. Rel.: Min. Luis Felipe Salomão, Data de Julgamento: 27/10/2009, Data de Publicação: 02/09/2009. Disponível em: [https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num\\_registro=200600946957](https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=200600946957). Acesso em: 22 fev. 2022.

BRASIL. Supremo Tribunal de Justiça (4ª Turma). **Recurso Especial n. 1168547/RJ**. Direito Processual Civil. Recurso Especial. Ação de indenização por utilização indevida de imagem em sítio eletrônico. Prestação de serviço para empresa espanhola. Contrato com cláusula de eleição de foro no exterior. Recorrente: World Company Dance Show LTDA. Recorrido: Patrícia Chélida de Lima Santos. Rel.: Min. Luis Felipe Salomão, Data de Julgamento: 11/05/2010, Data de Publicação: 07/02/2011. Disponível em: [https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num\\_registro=200702529083](https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=200702529083). Acesso em: 22 fev. 2022.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Inquérito n. 4781 Ref/DF**. Penal e Processo Penal. Não incidência de inviolabilidade parlamentar (CF, art. 53, *caput*). Possibilidade constitucional de prisão em flagrante delito de deputado federal pela prática de crime inafiançável (CF, artigo 53, §2º). Necessidade da Câmara dos Deputados deliberar sobre sua manutenção. Decisão referendada. Rel.: Min. Alexandre de Moraes, Data de Julgamento: 17/02/2021, Data de Publicação: 14/05/2021. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur446255/false>. Acesso em: 22 fev. 2022.

BUCHANAN, Allen. Human nature and enhancement. **Bioethics**, Hoboken, v. 23, n. 3, 21 jan. 2009. DOI 10.1111/j.1467-8519.2008.00633.

CAPEZ, Fernando. **Curso de Processo Penal**. 19. ed. São Paulo: Saraiva, 2012.

CASSIRER, Ernest. **Filosofia das formas simbólicas: 1 - A linguagem**. Tradução: Marion Fleischer. 1. ed. São Paulo: Martins Fontes, 2001. Título original: Philosophie der symbolischen formen – die Sprache. v. 1.

CASTELLS, Manuel. **A Galáxia da Internet: Reflexões sobre a Internet, os negócios e a sociedade**. Tradução: Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003. Título original: The Internet Galaxy: Reflections on the Internet, Business and Society.

CASTELLS, Manuel. Communication, power and counter-power in the network society. **International Journal of Communication**, Los Angeles, v. 1, p. 238-266, 2007. DOI 1932-8036/20070238.

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. **The New York Times**, New York, 04 Apr. 2018. Politics. Disponível em: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. Acesso em: 20 jun. 2022.

COSTA, Daniel Moraes da. **Boas Práticas para Perícia Forense**. 2008. 44 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Centro Universitário de Jaguariúna, UniFAJ, Jaguariúna, 2008.

COSTA, José Augusto Fontoura. Contratação No Ambiente Digital: Mudanças Profundas Ou Superficiais?. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 4, jul./set. 2019.

CPI – CRIMES CIBERNÉTICOS. **Relatório Final**. Brasília, DF: Câmara Dos Deputados, 04 maio 2016. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos>. Acesso em: 16 jun. 2022.

CROWD RESEARCH. Insider Treat Report 2019. **Cybersecurity Insiders**, Baltimore, 2019. Portfolio. Disponível em: <https://www.cybersecurity-insiders.com/portfolio/insider-threat-report/>. Acesso em: 25 jan. 2022.

DARWIN, Charles. **The Origin of Species: by Means of Natural Selection, Preservation of Favoured Races in the Struggle for Life**. London: John Murray, 1859.

DASCALESCU, Ana. 10 Alarming Cyber Security Facts that Threaten Your Data. **Heimdall Security**, Copenhagen, 29 Mar. 2018. Blog. Disponível em: <https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/>. Acesso em: 12 fev. 2022.

DINIZ, Maria Helena. **Tratado teórico e prático dos contratos**. 6. ed. São Paulo: Saraiva, 2006. v. 5

DISTRITO FEDERAL. Tribunal de Justiça (2ª Turma Recursal dos Juizados Especiais Cíveis e Criminais do DF). **Apelação Cível no Juizado Especial n. 2006.01.1.096659-8**. Transação comercial. Site especializado da internet. Prestação de serviço. Fraude. Captura de informações pessoais do cadastro. Culpa exclusiva de terceiro afastada. Risco decorrente da exploração da atividade econômica. Apelante: Mercadolivre.com Atividades de Internet LTDA. Apelado: Andressa Suemy Honjoya. Rel.: Juiz Luis Gustavo B. de Oliveira, Data de Julgamento: 18/03/2008, Data de Publicação: 29/04/2008. Disponível em: <https://pesquisajuris.tjdft.jus.br/>. Acesso em: 25 jan. 2022.

DONEDA, Danilo. O direito fundamental à proteção de dados. In: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. 1. ed. São Paulo: Atlas, 2014.

EKMAN, Pedro; BARBOSA, Bia. Regulação da mídia não é censura. **CartaCapital**, São Paulo, 03 jun. 2014. Entrevistas. Disponível em: <https://www.cartacapital.com.br/blogs/intervozes/regulacao-da-midia-nao-e-censura-2340/>. Acesso em: 20 fev. 2022.

ELLUL, Jacques. **A Técnica e o Desafio do Século**. Tradução: Roland Corbisier. Rio de Janeiro: Paz e Terra, 1968. Título original: La Technique ou L'enjeu du Siècle.

ELLUL, Jacques; CHARBONNEAU, Bernard. Diretivas para um manifesto personalista. Tradução: Fernanda Elias. **Espiritualidade libertária**, São Paulo, n. 3, p. 136-168, 1. sem. 2011. Título original: Les années personnalistes. Disponível em: [https://espiritualidadelibertaria.files.wordpress.com/2011/07/09\\_n3\\_charbonneau\\_ellul.pdf](https://espiritualidadelibertaria.files.wordpress.com/2011/07/09_n3_charbonneau_ellul.pdf). Acesso em: 22 jan. 2022.

ELLUL, Jacques. **The Technological Bluff**. Translation: Geoffrey W. Bromiley. Grand Rapids: Eerdmans Publishing Company, 1990. Título original: Le bluff technologique.

ELLUL, Jacques. **The Technological Society**. Translation: John Wilkinson. New York: Alfred A. Knopf, 1964. Título original: La Technique ou L'enjeu du Siècle.

EUROPEAN UNION. Court of Justice (Grand Chamber). **Joined Cases C-509/09 and C-161/10**. Regulation (EC) No 44/2001. Jurisdiction and the enforcement of judgments in civil and commercial matters. Jurisdiction 'in matters relating to tort, delict or quasi-delict'. Directive 2000/31/EC. Publication of information on the internet. Adverse effect on personality rights. Place where the harmful event occurred or may occur. Law applicable to information society services. Plaintiffs: eDate Advertising GmbH, Olivier Martinez and Robert Martinez. Defendants: X and MGN Limited. Document 62009CJ0509. Judgment Date: 25/10/2011. Luxembourg: EUR-Lex, 2011. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0509&qid=1622314428025>. Acesso em: 15 de maio de 2022.

EUROPEAN UNION. European Parliament. **Resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020: Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II')**, Case C-311/18 (2020/2789(RSP)). Document 52021IP0256. Luxembourg: EUR-Lex, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021IP0256&qid=1674253121309>. Acesso em: 28 mar. 2022.

EXPERIAN. 2015 Second Annual Data Breach Industry Forecast. **Experian**, Dublin, 2014. White Papers. Disponível em: <https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf>. Acesso em: 22 jan. 2022.

FONSECA, Flávia Regina Nápoles. **Marco Civil na Internet e a Virtualização da Empresa**. 2011. 119 f. Dissertação (Mestrado em Direito Empresarial) – Curso de Pós-Graduação Stricto Sensu, Faculdade de Direito Milton Campos, Nova Lima, 2011.

FRANSSEN, Maarten; LOKHORST, Gert-Jan; VAN DE POEL, Ibo. Philosophy of Technology. **The Stanford Encyclopedia of Philosophy Archive**, Palo Alto, 06 Sept. 2018. Technology. Disponível em: <https://plato.stanford.edu/archives/fall2018/entries/technology/>. Acesso em: 19 jan. 2022.

FUKUYAMA, Francis. **Our posthuman future: consequences of the biotechnology revolution**. New York: Farrar, Straus and Giroux, 2002.

GALVÃO, Helder. Plágio e Internet. In: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. 1. ed. São Paulo: Atlas, 2014.

GARCIA, Daiene Kelly. O Pensamento de Jacques Ellul e Uso das Novas Tecnologias na Veiculação da Publicidade: a Alienação como Instrumento da Técnica. In: IV SEMINÁRIO BRASILEIRO SOBRE O PENSAMENTO DE JACQUES ELLUL, 4. ed., 2011, Rio de Janeiro. **Anais do IV Seminário Brasileiro sobre o pensamento de Jacques Ellul**. Rio de Janeiro: Faculdade Nacional de Direito, 2011.

GEMALTO. Breach Level Index. **Gemalto**, Paris, 09 Oct. 2018. Enterprise Security. Disponível em: <https://blog.gemalto.com/security/2018/10/09/breached-records-more-than-doubled-in-h1-2018-reveals-breach-level-index/>. Acesso em: 22 jan. 2022.

GERALDINO, Maria Carolina Tavares. **Liberdade de Expressão x Direito à Privacidade e à Honra: uma perspectiva à luz da Internet**. 2012. 30 f. Artigo Científico (Especialização em Direito) – Curso de Pós-Graduação do Estado do Rio de Janeiro, Escola de Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2012.

GERMANY. Federal Constitutional Court (First Division). **BVerfGE 35, 202**: Lebach. Petitioner: Lebach. Judgment date: 05 June 1973. Translation: F. H. Lawson and B. S. Markesinis. Berlin: German Law Archive, 1999. Disponível em: <https://germanlawarchive.iuscomp.org/?p=62>. Acesso em: 07 jun. 2022.

GOMES, Orlando Gomes. **Contrato de Adesão: Condições Gerais dos Contratos**. São Paulo: Revista dos Tribunais, 1972.

GREENBERG, Andy. An Interview With The Hacker Probably Selling Your Password Right Now. **Wired**, New York, 09 June 2016. Security. Disponível em: <https://www.wired.com/2016/06/interview-hacker-probably-selling-password/>. Acesso: 06 jun. 2022.

HABERMAS, Jürgen. **Legitimation Crisis**. Translation: Thomas McCarthy. Boston: Beacon Press, 1975. Título original: Legitimationsprobleme im Spätkapitalismus.

HABERMAS, Jürgen. **O futuro da natureza humana**: a caminho de uma eugenia liberal?. Tradução: Karina Jannini. São Paulo: Martins Fontes, 2004. Título original: Die Zukunft Der Menschlichen Natur: Auf dem Weg zu einer liberalen Eugenik?.

HABERMAS, Jürgen. The Constitutionalization of International Law and the Legitimation Problems of a Constitution for World Society. Translation: Ciaran Cronin. **Constellations**, Hoboken, v. 15, n. 4, p. 444-455, 11 Nov. 2008. Título original: Konstitutionalisierung des Völkerrechts und Internationalisierung des Verfassungsrechts. DOI 10.1111/j.1467-8675.2008.00510.

HARDIN, Garrett. **A Tragédia dos Comuns**. Tradução: José Roberto Bonifácio. Rio de Janeiro: UGF, 2011. Título original: The Tragedy of the Commons.

HASBINI, Mohamad Amin. 5g Technology Predictions 2020. **Secure List**, London, 03 Dec. 2019. Kaspersky Security Bulletin. Disponível em: <https://securelist.com/5g-predictions-2020/95386/>. Acesso em: 29 jan. 2022.

HEIDEGGER, Martin. **El Origen de la Obra de Arte**. Traducción: Helena Cortés y Arturo Leyte. Madrid: Alianza, 1996. Título original: Der Ursprung des Kunstwerkes.

HEIDEGGER, Martin. **The Question concerning Technology and Other Essays**. Translation: Villiam Lovitt. New York: Harper and Row, 1977. Título original: Die Frage nach der Technik.

HEIM, Patrick. Resetting passwords to keep your files safe. **Dropbox**, São Francisco, 25 Aug. 2016. Company. Disponível em: <https://blogs.dropbox.com/dropbox/2016/08/resetting-passwords-to-keep-your-files-safe/>. Acesso em: 12 fev. 2022.

HELD, David; MAFFETONE, Pietro. Legitimacy and Global Governance. In: HELD, David; MAFFETONE, Pietro (ed.). **Global Political Theory**. Cambridge: Polity, 2016.

HILL, Kashmir; MATTU, Surya. Facebook Knows How to Track You Using the Dust on Your Camera Lens. **Gizmodo**, New York, 11 Jan. 2018. Disponível em: <https://gizmodo.com/facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620>. Acesso em: 10 fev. 2022.

HOBBS, Thomas. **Leviatã**: matéria, forma e poder de um estado eclesiástico e civil. Tradução: João Paulo Monteiro e Maria Beatriz Nizza da Silva. São Paulo: Martins Fontes, 2003. Título original: Leviathan or The Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil.

HORWITZ, Jeff. The Facebook Files: A Wall Street Journal investigation. **The Wall Street Journal**, New York, 05 Oct. 2021. Articles. Disponível em: <https://www.wsj.com/articles/the-facebook-files-11631713039>. Acesso em: 17 jan. 2023.

HPE SECURITY RESEARCH. Cyber Risk Report 2016. **Hewlett Packard Enterprise (HPE)**, Spring, 09 June 2016. Software solutions. Disponível: [https://securitydelta.nl/media/com\\_hsd/report/57/document/4aa6-3786enw.pdf](https://securitydelta.nl/media/com_hsd/report/57/document/4aa6-3786enw.pdf). Acesso em: 12 fev. 2022.

HUGHES, Thomas Parke. **American Genesis: A Century of Invention and Technological Enthusiasm, 1870-1970**. 2nd ed. Chicago: University of Chicago Press, 2004.

HUGHES, Thomas Parke. **Human-Built World: How to Think about Technology and Culture**. Chicago: University of Chicago Press, 2005.

HUMANITY+. The Transhumanist Declaration. **Humanity+**, Los Angeles, Mar. 2009. Disponível em: <https://www.humanityplus.org/the-transhumanist-declaration>. Acesso em: 04 fev. 2022.

HUNT, Troy. The 773 Million Record “Collection #1” Data Breach. **TroyHunt**, Surfers Paradise, 17 Jan. 2019. Disponível em: <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>. Acesso em: 19 jan. 2022.

IBM SECURITY. Cost of a Data Breach Report 2019. **IBM**, Armonk, July 2019. Reports. Disponível em: <https://www.ibm.com/downloads/cas/RDEQK07R>. Acesso em: 25 jan. 2022.

IFPI. Global Music Report 2018: State of the Industry. **IFPI**, London, 24 Apr. 2018. News. Disponível em: <https://www.fimi.it/kdocs/1922703/gmr-2018-ilovepdf-compressed.pdf>. Acesso em: 12 jun. 2022.

IHDE, Don. **Existential Technics**. Albany: SUNY Press, 1983.

IHDE, Don. **Technology and the Lifeworld**. Bloomington: Indiana University Press, 1990.

JESUS, Damásio de. **Direito Penal**. 30. ed. São Paulo: Saraiva, 2009. v. 1

JOHNSON, Deborah G.; WAYLAND, Kent A. Surveillance and transparency as sociotechnical systems of accountability. In: HAGGERTY, Kevin D.; SAMATAS, Minas. **Surveillance and democracy**. London: Routledge, 2010.

JUNIPER RESEARCH. **The Future of Cybercrime & Security**. Hampshire: Juniper Research, 2019.

KAPLAN, David M. **Ricoeur’s Critical Theory**. New York: State University of New York Press, 2003.

KASPERSKY LAB. Are you cyber savvy?: Research Summary. **Kaspersky**, London, 22 Sept. 2015. Corporate News. Disponível em: [https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234157/Cyber\\_savvy\\_quiz\\_report.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234157/Cyber_savvy_quiz_report.pdf). Acesso em: 22 jan. 2022.

KASPERSKY LAB. Kaspersky Security Bulletin 2019: Advanced threat predictions for 2020. **Secure List**, London, 20 Nov. 2019a. Kaspersky Security Bulletin. Disponível em: <https://securelist.com/advanced-threat-predictions-for-2020/95055/>. Acesso em: 25 jan. 2022.

KASPERSKY LAB. Kaspersky Security Bulletin 2019: Statistics. **Secure List**, London, 12 Dec. 2019b. Kaspersky Security Bulletin. Disponível em: <https://securelist.com/kaspersky-security-bulletin-2019-statistics/95475/>. Acesso em: 25 jan. 2022.

KASPERSKY LAB. Story of the year 2019: Cities under ransomware siege. **Secure List**, London, 11 Dec. 2019c. Kaspersky Security Bulletin. Disponível em: <https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/>. Acesso em: 29 jan. 2022.

KASPERSKY LAB. The Human Factor in IT Security. **Kaspersky**, London, 10 July 2017. Press Releases. Disponível em: [https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083900/20170710\\_Report\\_Human-Factor-In-ITSec\\_eng\\_final.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083900/20170710_Report_Human-Factor-In-ITSec_eng_final.pdf). Acesso em: 22 jan. 2022.

KREBS, Brian. First American Financial Corp. Leaked Hundreds of Title Insurance Records. **KrebsOnSecurity**, Arlington, 24 May 2019. Disponível em: <https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/>. Acesso em: 29 jan. 2022.

LEITE, Taylisi de Souza Corrêa. A Palavra Humilhada e a Construção Técnica da Ideologia pela Indústria Cultural: uma Visão Crítica sobre a Televisão. In: BARRIENTOS-PARRA, Jorge David; MATOS, Marcus Vinicius A. B. (org.). **Direito, Técnica e Imagem: Os Limites e os Fundamentos do Humano**. São Paulo: Cultura Acadêmica, 2013.

LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez de Oliveira, 2005.

LEONARDI, Marcel. **Tutela da privacidade na internet**. 2009. 344 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

LESSIG, Lawrence. **Code and other Laws of Cyberspace**. New York: Basic Books, 1999.

LIMA, Cíntia Rosa Pereira de. **Validade e obrigatoriedade dos contratos de adesão eletrônicos (shrink-wrap e click-wrap) e dos termos e condições de uso (browse-wrap): Um estudo comparado entre Brasil e Canadá**. 2009. 701 f. Tese (Doutorado em Direito Civil) – Programa de Pós-Graduação em Direito, Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

LIMA, Renato Brasileiro de. **Curso de Processo Penal**. Niterói: Impetus, 2013.

LUHMANN, Niklas. **Trust and Power**. Translation: Howard Davis, John Raffan and Kathryn Rooney. Chichester: Wiley, 1979. Título original: Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität.

MADALENA, Juliano. Regulação das Fronteiras da Internet: um primeiro passo para uma teoria geral do Direito Digital. **Revista dos Tribunais**, São Paulo, v. 105, n. 974, p. 81-110, dez. 2016. Disponível em: <https://dspace.almg.gov.br/retrieve/111736/Juliano%20Madalena.pdf>. Acesso em: 22 jan. 2022.

MARQUES, Cláudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor**. São Paulo: Revista dos Tribunais, 2004.

MARSH. 2019 Global Cyber Risk Perception Survey: Insights. **Microsoft**, Redmond, Sept. 2019. Security. Disponível em: <https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>. Acesso em: 25 jan. 2022.

MARX, Karl. **Das Kapital**: Kritik der politischen Ökonomie. Hamburg: Verlag von Otto Meissner, 1867.

MATRIX Reloaded. Direção e Roteiro: Lilly Wachowski e Lana Wachowski. Produção: Joel Silver. Produtores: Village Roadshow Pictures, NPV Entertainment e Silver Pictures. Distribuição: Columbia Pictures e Roadshow Entertainment. Nova Iorque: HBOMax, 23 maio 2003. 2hrs18min, son., color. Acesso em: 4 fev. 2022.

MATSUURA, Sérgio; JANSEN, Thiago. Onda de crimes praticados por hackers cresceu 197% no Brasil em um ano. **O Globo**, Rio de Janeiro, 16 ago. 2015. Economia. Disponível em: <https://oglobo.globo.com/economia/onda-de-crimes-praticados-por-hackers-cresceu-197-no-brasil-em-um-ano-17197361>. Acesso em: 12 fev. 2022.

MATTEUCCI, Nicola. Estado Contemporâneo. In: BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. **Dicionário de Política**. 11. ed. Brasília, DF: Universidade de Brasília, 1998.

MCAFEE LABS. Threats Report: august 2015. **McAfee**, San José, 01 Sept. 2015. Reports. Disponível em: <http://www.mcafee.com/es/resources/reports/rp-quarterly-threats-aug-2015.pdf>. Acesso em: 19 fev. 2019.

MCLUHAN, Marshall. **Os meios de comunicação**: como extensões do homem. 8. ed. São Paulo: Cultrix, 1996.

MESTHENE, Emmanuel G. **Technological Change**: It's Impact on Man and Society. Cambridge: Harvard University Press, 1970.

MEUCCI, Arthur. O pensamento liberal e a proibição da publicidade infantil. **Revista Espaço Ético**: Educação, Gestão e Consumo, São Paulo, a. 2, v. 1, n. 6, p. 77-82, set./dez. 2015.

MILL, John Stuart. **A Liberdade/Utilitarismo**. Tradução: Eunice Ostrensky. São Paulo: Martins Fontes, 2000. Título original: On Liberty.

MINAS GERAIS. Tribunal de Justiça (16ª Câmara Cível). **Apelação Cível n. 1.0056.11.003473-5/002**. Apelação Cível. Ação de Cobrança. Contrato eletrônico. Princípio da Equivalência Funcional. Prova da assinatura. Art. 389, II do CPC. Ausência de demonstração. Sentença mantida. Apelante: Itaú Unibanco Holding S/A nova denominação de Banco Itaú S/A, decorrente de fusão. Apelado: João Penna Esteves. Rel.: Des. José Marcos Vieira, Data de Julgamento: 03/07/2013, Data de Publicação: 12/07/2013. Disponível em: <https://www5.tjmg.jus.br/jurisprudencia/pesquisaNumeroCNJEspelhoAcordao.do?numeroRegistro=1&totalLinhas=1&linhasPorPagina=10&numeroUnico=1.0056.11.003473-5%2F002&pesquisaNumeroCNJ=Pesquisar>. Acesso em: 22 jan. 2022.

MITCHAM, Carl. **Thinking through Technology**: The Path between Engineering and Philosophy. Chicago: University of Chicago Press, 1994.

MOCELLIN, Vanessa Delazeri. **O ser da técnica conforme Martin Heidegger e Jacques Ellul**. 2012. 179 f. Dissertação (Mestrado em Filosofia) – Programa de Pós-Graduação em Filosofia, Centro de Filosofia e Ciências Humanas, Universidade Federal de Santa Catarina, Florianópolis, 2012.

MOKYR, Joel. **The Lever of Riches**: Technological Creativity and Economic Progress. Oxford: Oxford University Press, 1992.

MONTEIRO, Fábio. Como funciona a internet na Coreia do Norte. **Observador**, Lisboa, 23 dez. 2014. Crime Informático. Disponível em: <http://observador.pt/2014/12/23/como-funciona-internet-na-coreia-norte/>. Acesso em: 10 fev. 2022.

MORALES VILHA, Anapátricia. **E-marketing para bens de consumo durável**. Rio de Janeiro: Editora FGV, 2002.

NEUMANN, Franz. **Lo Stato democratico e lo Stato autoritário**. Bologna: Il Mulino, 1973.

NEVES, Marcelo. **Transconstitucionalismo**. São Paulo: WMF Martins Fontes, 2009.

NICHOLS, Sam. Your Phone Is Listening and it's Not Paranoia. **Vice**, New York, 04 June 2018. Motherboard. Disponível em: <https://www.vice.com/en/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia>. Acesso em: 10 fev. 2022.

NIETZSCHE, Friedrich. **Assim Falava Zaratustra**: um Livro para Todos e para Ninguém. Tradução: José Mendes de Souza. Jul. 2002. *E-book*. Título original: Also sprach Zarathustra: Ein Buch für Alle und Keinen. Disponível em: <http://www.ebooksbrasil.org/eLibris/zara.html>. Acesso em: 12 fev. 2022.

NORTON. Norton Cyber Security 2012. **Norton**, Tempe, 01 Sept. 2012. Press Releases. Disponível em: [https://biz-file.com/f/1311/2012\\_Norton\\_Cybercrime\\_Report\\_.pdf](https://biz-file.com/f/1311/2012_Norton_Cybercrime_Report_.pdf). Acesso em: 12 fev. 2022.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14. ed. São Paulo: Revista dos Tribunais, 2014.

NUNES, Vidal S. A publicidade comercial direcionada ao público infantil. In: MARTINS, Ives Gandra; REZEK, Francisco. **Constituição Federal**: avanços, contribuições e modificações no processo democrático brasileiro. São Paulo: Revista dos Tribunais, 2008.

OBERMEYER, Ziad *et al.* Dissecting racial bias in an algorithm used to manage the health of populations. **Science**, Washington, v. 366, issue 6464, p. 447-453, 25 Oct. 2019. DOI 10.1126/science.aax2342.

OFFE, Claus. **Contradictions of the Welfare State**. Edition: John Keane. London: Hutchinson & Co. Ltd., 1984.

OLIVO, Luis Carlos Cancellier. **Direito e Internet**: a regulamentação do Ciberespaço. 2. ed. Florianópolis: Editora UFSC, 1998.

ORTEGA Y GASSET, José. **A Rebelião das Massas**. Tradução: Herrera Filho. Edição: Ridendo Castigat Mores. 07 nov. 2001. *E-book*. Título Original: La rebelión de las masas. Disponível em: [http://www.dominiopublico.gov.br/pesquisa/DetalheObraDownload.do?select\\_action=&coobra=2291&co\\_midia=2](http://www.dominiopublico.gov.br/pesquisa/DetalheObraDownload.do?select_action=&coobra=2291&co_midia=2). Acesso em: 22 jan. 2022.

PARÁ. Tribunal de Justiça (3ª Câmara Cível Isolada). **Agravo de Instrumento, Acórdão n. 47062**. Contratos de acesso à internet. Relação de consumo. Foro competente. Lugar onde ocorreu o dano. Contratos de prestação de serviços que tem por objeto principal o acesso à internet, com ou sem licenciamento de programas, em caráter individualizado e contínuo, a título oneroso ou gratuito, por prazo determinado ou indeterminado, são considerados como de consumo e sujeitos ao foro do lugar do consumidor lesado. Votação unânime, recurso improvido. Rel.: Des. Marta Inês Antunes Jadão, Data de Julgamento: 17/10/02, Data de publicação: 23/10/02. Disponível em: <https://gsa-index.tjpa.jus.br/consultas/>. Acesso em: 19 jan. 2019.

PARANAGUÁ, Pedro; BRANCO, Sérgio. **Direitos Autorais**. Rio de Janeiro: FGV, 2009.

PERLROTH, Nicole. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. **The New York Times**, New York, 03 Oct. 2017. Technology. Disponível em: <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>. Acesso em: 29 jan. 2022.

PERLROTH, Nicole; TSANG, Amie; SATARIANO, Adam. Marriott Hacking Exposes Data of Up to 500 Million Guests. **The New York Times**, New York, 30 Nov. 2018. Business. Disponível em: <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html>. Acesso em: 29 jan. 2022.

PERSSON, Ingmar; SAVULESCU, Julian. Moral transhumanism. **Journal of Medicine and Philosophy**, Oxford, v. 35, issue 6, p. 656-669, 12 Dec. 2010. DOI 10.1093/jmp/jhq052.

PICOLO, Jéssica de Freitas. **Criminologia em torno do crime cibernético**. 2015. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Direito, Faculdades Integradas de Santa Fé do Sul, Santa Fé do Sul, 2015.

PINHEIRO, Patrícia Peck. **Direito Digital**. 3. ed. São Paulo: Saraiva, 2009.

PITOMBO, Cleunice A. **Da Busca e da Apreensão no Processo Penal**. 2. ed. São Paulo: Revista dos Tribunais, 2005.

PONEMON INSTITUTE. 2018 Ponemon Study on Global Megatrends in Cybersecurity. **Ponemon Institute**, Traverse City, 15 Mar. 2018. Security. Disponível em: <https://www.ponemon.org/news-updates/blog/security/ponemon-institute-announces-the-release-of-the-2018-megatrends-study.html>. Acesso em: 22 jan. 2019.

PONEMON INSTITUTE. Global Trends in Identity Governance & Access Management. **Ponemon Institute**, Traverse City, 21 Sept. 2016. Security. Disponível em: [https://www.netiq.com/docrep/documents/jghd2o5rqw/micro\\_focus\\_consolidated\\_report.PDF](https://www.netiq.com/docrep/documents/jghd2o5rqw/micro_focus_consolidated_report.PDF). Acesso em: 12 de jun. 2022.

PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de Direito Privado**. São Paulo: Revista dos Tribunais, 2012.

QUEDA Livre. In: **Black Mirror**. Criação: Charlie Brooker. Roteiristas: Michael Schur e Rashida Jones. Direção: Joe Wright. Realização, Distribuição e Produção: Netflix. Londres: Endemol UK, 21 out. 2016. 49min, son., color. Primeiro episódio da terceira temporada da série. Acesso em: 4 fev. 2022.

RIO DE JANEIRO (Estado). Tribunal de Justiça (5ª Câmara Cível). **Apelação Cível n. 0103911-74.2010.8.19.0001**. Responsabilidade Civil. Relação de consumo. Ação de Obrigação de Fazer c/c Indenizatória. Comércio eletrônico. Alegação de veiculação de propaganda com preço promocional não comprovada. Erro evidente do preço. Princípio da Boa-fé Objetiva que exige um comportamento leal de ambas as contratantes. Partes condenação por litigância de má-fé que se afasta. Provimento parcial do recurso. Apelante: Anderson de Souza Ferreira. Apelado: B2W Companhia Global do Varejo. Rel.: Claudia Telles de Menezes, Data de Julgamento: 15/02/2011, Data de Publicação: 16/02/2011. Disponível em: <https://www3.tjrj.jus.br/ejud/ConsultaProcesso.aspx?N=2010.001.81891>. Acesso em: 22 jan. 2022.

RIO DE JANEIRO (Estado). Tribunal de Justiça (27ª Câmara Cível). **Apelação Cível n. 0450891-64.2014.8.19.0001**. Apelação. Ação cautelar de exibição de documentos. Relatório de “logs de IP” dos acessos efetuados à conta de correio eletrônico. Legitimidade passiva. [...] Honorários advocatícios de sucumbência reduzidos a um mil reais. Parcial provimento do recurso. Apelante: Microsoft Informática LTDA. Apelado: Diniz Rodrigues Teixeira Casanova. Rel.: Des. Maria Luiza de Freitas Carvalho, Data de Julgamento: 13/07/2016, Data da Publicação: 18/07/2016. Disponível em: <https://www3.tjrj.jus.br/ejud/ConsultaProcesso.aspx?N=2016.001.15038>. Acesso em: 22 jan. 2022.

RIO GRANDE DO SUL. Tribunal de Justiça (1ª Turma Recursal Cível). **Recurso Inominado n. 71002088896**. Recurso Inominado. Consumidor. Comércio eletrônico. Aquisição de produto através de acesso a rede mundial de computadores (internet). Notebook adquirido no site da co-ré Buscapé. Produto não entregue. Indicação de confiabilidade da empresa vendedora pela co-requerida UOL. Responsabilidade solidária. Sentença de procedência. [...] Sentença mantida. Recursos improvidos. Recorrentes: Buscapé Informação e Tecnologia LTDA e Universo Online S.A. Recorridos: Calinca Boniatti e Tray Locações de Sistemas de Internet LTDA. Rel.: Dr. Leandro Raul Klippel, Data de Julgamento: 19/11/2009, Data de Publicação: 25/11/2009a. Disponível em: [https://www.tjrs.jus.br/site\\_php/consulta/consulta\\_processo.php?nome\\_comarca=Turmas%20Recursais&versao=&versao\\_fonetica=1&tipo=1&id\\_comarca=700&num\\_processo\\_mask=&num\\_processo=71002088896&codEmenta=7706337&temIntTeor=true](https://www.tjrs.jus.br/site_php/consulta/consulta_processo.php?nome_comarca=Turmas%20Recursais&versao=&versao_fonetica=1&tipo=1&id_comarca=700&num_processo_mask=&num_processo=71002088896&codEmenta=7706337&temIntTeor=true). Acesso em: 25 jan. 2022.

RIO GRANDE DO SUL. Tribunal de Justiça (2ª Turma Recursal Cível). **Recurso Inominado n. 71002058915**. Cominatória. Consumidor. Comércio eletrônico. Aquisição de computador por preço promocional. Pedido cancelado sob argumento de erro momentâneo no site. No caso em tela, a oferta não vincula o fornecedor, diante do erro substancial da publicação, perceptível pelo homem médio diante da desarrazoabilidade do valor ofertado. Princípios da boa-fé e do equilíbrio (art. 4º, III, do CDC). Recurso provido para julgar improcedente o pedido do autor. Recorrente: Dell Computadores do Brasil LTDA. Recorrido: Edgar Zavareze

da Silva. Rel.: Juiz Afif Jorge Simões Neto, Data de Julgamento: 02/12/2009, Data de Publicação: 07/12/2009b. Disponível em:  
[https://www.tjrs.jus.br/site\\_php/consulta/consulta\\_processo.php?nome\\_comarca=Turmas%20Recursais&versao=&versao\\_fonetica=1&tipo=1&id\\_comarca=700&num\\_processo\\_mask=&num\\_processo=71002058915&codEmenta=7706337&temIntTeor=true](https://www.tjrs.jus.br/site_php/consulta/consulta_processo.php?nome_comarca=Turmas%20Recursais&versao=&versao_fonetica=1&tipo=1&id_comarca=700&num_processo_mask=&num_processo=71002058915&codEmenta=7706337&temIntTeor=true). Acesso em: 25 jan. 2022.

RIO GRANDE DO SUL. Tribunal de Justiça (2ª Turma Recursal Cível). **Recurso Inominado n. 71002292050**. Compra e venda. Comércio eletrônico. Responsabilidade do site. O site que simplesmente efetua a divulgação de determinada loja eletrônica não é responsável por eventuais falhas nos contratos de aquisição. Afastada, assim, a responsabilidade do site eis não existir qualquer elemento que possa indicar que possua interferência na relação de consumo. Inexistente a entrega do produto pelo fornecedor a circunstância não permite a caracterização de dano moral indenizável. Ausente qualquer agressão a atributos da personalidade. Negado provimento ao recurso do autor e provido o recurso da ré TERRA. Recorrente/recorrido: Terra Networks Brasil S/A. Recorrido/Recorrente: Carlos Alfredo Franklin de Vargas. Recorridos: Antonio Carlos de Sá Oliveira e Informática ME – ACO. Rel.: Dr. Eduardo Kraemer, Data de Julgamento: 17/12/2010, Data de Publicação: 12/01/2011. Disponível em:  
[https://www.tjrs.jus.br/site\\_php/consulta/consulta\\_processo.php?nome\\_comarca=Turmas%20Recursais&versao=&versao\\_fonetica=1&tipo=1&id\\_comarca=700&num\\_processo\\_mask=&num\\_processo=71002292050&codEmenta=7706337&temIntTeor=true](https://www.tjrs.jus.br/site_php/consulta/consulta_processo.php?nome_comarca=Turmas%20Recursais&versao=&versao_fonetica=1&tipo=1&id_comarca=700&num_processo_mask=&num_processo=71002292050&codEmenta=7706337&temIntTeor=true). Acesso em: 25 jan. 2022.

RIO GRANDE DO SUL. Tribunal de Justiça (3ª Turma Recursal Cível). **Recurso Inominado n. 71000650705**. Consumidor. Oferta. Vinculação. Erro. Preço irrisório de bem de consumo. Ar condicionado de 30.000 btus oferecido na rede da internet, no site da loja Submarino.com pelo valor de R\$ 3,00. Aplicável à espécie os princípios da boa-fé, equilíbrio e a vedação ao enriquecimento sem causa, os quais afastam a obrigatoriedade da oferta constante do art. 30 e 35, inciso I, do CDC. Recurso provido. Recorrente: Submarino S/A. Recorrido: Felipe Silveira Ramos. Rel.: Dra. Maria José Schmitt Santanna, Data de Julgamento: 31/05/2005, Data de Publicação: 17/06/2005. Disponível em:  
[https://www.tjrs.jus.br/site\\_php/consulta/consulta\\_processo.php?nome\\_comarca=Turmas%20Recursais&versao=&versao\\_fonetica=1&tipo=1&id\\_comarca=700&num\\_processo\\_mask=&num\\_processo=71000650705&codEmenta=7706337&temIntTeor=true](https://www.tjrs.jus.br/site_php/consulta/consulta_processo.php?nome_comarca=Turmas%20Recursais&versao=&versao_fonetica=1&tipo=1&id_comarca=700&num_processo_mask=&num_processo=71000650705&codEmenta=7706337&temIntTeor=true). Acesso em: 25 jan. 2022.

RIO GRANDE DO SUL. Tribunal de Justiça (9ª Câmara Cível). **Apelação Cível n. 70068005966**. Apelação Cível. Responsabilidade Civil. Ação de Indenização por Danos Morais. Google Brasil Internet LTDA. Criação de blog difamatório no Google Espanha. possibilidade de reclamação à filial brasileira do google. competência da justiça brasileira. extensão. Informações injuriosas mantidas mesmo após a “denúncia de abuso” relatada pela autora. Danos morais configurados. Quantum mantido. Impugnação à AJG. Acolhimento. [...] Preliminar desacolhida, agravo retido desprovido e apelo parcialmente provido. Apelante: Google Brasil. Apelado: Marluse Giusto. Rel.: Des. Eugênio Facchini Neto, Data de Julgamento: 27/04/2016, Data de Publicação: 05/05/2016. Disponível em:  
[https://www.tjrs.jus.br/site\\_php/consulta/consulta\\_processo.php?nome\\_comarca=Tribunal%20de%20Justi%C3%A7a%20do%20RS&versao=&versao\\_fonetica=1&tipo=1&id\\_comarca=700&num\\_processo\\_mask=&num\\_processo=70068005966&codEmenta=7706337&temIntTeor=true](https://www.tjrs.jus.br/site_php/consulta/consulta_processo.php?nome_comarca=Tribunal%20de%20Justi%C3%A7a%20do%20RS&versao=&versao_fonetica=1&tipo=1&id_comarca=700&num_processo_mask=&num_processo=70068005966&codEmenta=7706337&temIntTeor=true). Acesso em: 25 jan. 2022.

ROSEN, Guy. Security Update. **Facebook**, Melon Park, 28 Sept. 2018. Meta. Disponível em: <https://about.fb.com/news/2018/09/security-update/>. Acesso em: 29 jan. 2022.

SAFERNET BRASIL. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. **Safernet Brasil**, Salvador, 2018. Indicadores. Disponível em: <http://indicadores.safernet.org.br/>. Acesso em: 29 jan. 2022.

SALES, Fábio Augusto Cornazzani; LIMA, Gisele Truzzi de; MIRANDA, Rodrigo Barros de. Privacidade e Internet. **Revista de Direito das Novas Tecnologias**, São Paulo, v. 3, n. 1, jan. 2007. Disponível em: [https://www.truzzi.com.br/wp-content/uploads/2020/07/Artigo2\\_PrivacidadeInternet\\_GiseleTruzzi.pdf](https://www.truzzi.com.br/wp-content/uploads/2020/07/Artigo2_PrivacidadeInternet_GiseleTruzzi.pdf). Acesso em: 12 fev. 2019.

SANDBERG, Anders. Morphological Freedom: Why We not just Want it, but Need it. **Alders Sandberg's pages**, Stockholm, 22 June 2001. NADA EECS KTH. Disponível em: <http://www.aleph.se/Nada/Texts/MorphologicalFreedom.htm>. Acesso em: 04 fev. 2022.

SANDVINE. The Global Internet Phenomena Report: October 2018. **Sandvine**, Waterloo, 02 Oct. 2018. Phenomena. Disponível em: <https://www.sandvine.com/hubfs/downloads/phenomena/2018-phenomena-report.pdf>. Acesso em: 26 abr. 2022.

SARLET, Ingo Wolfgang. A titularidade simultaneamente individual e transindividual dos direitos sociais analisada à luz do exemplo do direito à proteção e promoção da saúde. **Revista Brasileira de Direitos Fundamentais & Justiça**, Porto Alegre, v. 4, n. 10, p. 205-228, 30 mar. 2010. DOI 10.30899/dfj.v4i10.449.

SARMAH, Harshajit. Data Breach: Truecaller Exposes Indian Users' Data, Shows Cracks In Cyber Security Infrastructure. **Analytics India Magazine**, Bangaluru, 22 May 2019. Disponível em: <https://analyticsindiamag.com/data-breach-truecaller-exposes-indian-users-data-shows-cracks-in-cyber-security-infrastructure/>. Acesso em: 29 jan. 2022.

SÁVIO, Eduardo Borges. **A Responsabilidade Civil por Acidentes de Consumo no Comércio Eletrônico**. 2013. 88 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Direito, Universidade Federal de Goiás, Goiânia, 2013.

SCHURR, Amy. Get the Facts: Mobile App Breaches are Growing. **NowSecure**, Chicago, 06 Nov. 2019. Industry News. Disponível em: <https://www.nowsecure.com/blog/2019/11/06/get-the-facts-mobile-app-breaches-are-growing/>. Acesso em: 29 jan. 2022.

SECUREWORKS. 2016 Underground Hacker Marketplace Report. **SecureWorks**, Atlanta, 2016. Resources. Disponível em: <https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report>. Acesso em: 12 fev. 2022.

SELLARS, Wilfrid Stalker. Philosophy and the Scientific Image of Man. In: COLONDY, Robert (ed.). **Science, Perception, and Reality**. New York: Humanities Press/Ridgeview, 1962.

SILVEIRA, Newton. **Propriedade intelectual**: propriedade industrial, direito de autor, software, cultivares, nome empresarial, abuso de patentes. 5. ed. São Paulo: Manole, 2014.

SOUZA, Carlos Affonso Pereira de. Direitos autorais, tecnologia e transformações na criação e no licenciamento de obras intelectuais. *In*: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014.

SYMANTEC. 2018 Internet Security Threat Report: Executive Summary. **Symantec**, Mountain View, v. 23, Mar. 2018. ISTR. Disponível em: <https://docs.broadcom.com/doc/istr-23-executive-summary-en>. Acesso em: 22 jan. 2022.

SYMANTEC. 2019 Internet Security Threat Report: Executive Summary. **Symantec**, Mountain View, v. 24, Mar. 2019. ISTR. Disponível em: <https://docs.broadcom.com/doc/istr-24-executive-summary-en>. Acesso em: 22 jan. 2022.

SYMANTEC. Internet Security Threat Report 2015. **Symantec**, Mountain View, v. 20, Apr. 2015. ISTR. Disponível em: <https://docs.broadcom.com/doc/istr-15-april-volume-20-en>. Acesso em: 22 jan. 2022.

TALMADGE, Eric. North Korea now blocking Facebook, Twitter, other websites. **The Associated Press**, New York, 01 Apr. 2016. Articles. Disponível em: <https://apnews.com/article/128ede4fc729447ab4540a7438ce0175>. Acesso em: 10 fev. 2022.

TEIXEIRA, Tarcísio. **Direito Eletrônico**. São Paulo: Juarez de Oliveira, 2007.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**: e suas Repercussões no Direito Brasileiro. 2. tiragem. São Paulo: Thomson Reuters Brasil, 2019.

TEUBNER, Gunther. Globale Zivilverfassungen: Alternativen zur staatszentrierten Verfassungstheorie. **Zeitschrift Für Ausländisches Öffentliches Recht Und Völkerrecht**, München, v. 63, n. 1, 2003. Disponível em: [https://www.jura.uni-frankfurt.de/42828590/globale\\_zivilverfassungen.pdf](https://www.jura.uni-frankfurt.de/42828590/globale_zivilverfassungen.pdf). Acesso em: 22 jan. 2022.

TEUBNER, Gunther. The King's Many Bodies: The Self-Destruction of Law's Hierarchy. **Law & Society Review**, Hoboken, v. 31, n. 4, p. 763-788, 1997. DOI 10.2307/3053986.

THIERER, Adam. **Permissionless Innovation**: The Continuing Case for Comprehensive Technological Freedom. 2. ed. Arlington: Mercatus Center, 2016.

TRENDMICRO. A Global Black Market for Stolen Personal Data. **Trend Micro**, Irving, 2015. Security. Disponível em: <http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/>. Acesso em: 12 fev. 2022.

TROMP, Nynke; HEKKERT, Paul; VERBEEK, Peter-Paul. Design for Socially Responsible Behavior: A Classification of Influence Based on Intended User Experience. **Design Issues**, Cambridge, v. 27, issue 3, p. 3-19, 01 July 2011. DOI 10.1162/DESI\_a\_00087.

UNIÃO EUROPEIA. Tribunal de Justiça (Primeira Seção). **Processo C-292/10**. Competência judiciária e execução de decisões em matéria civil e comercial. Citação edital de documentos judiciais. Inexistência de domicílio ou paradeiro conhecido do demandado no território de um Estado-Membro. Competência “em matéria extracontratual”. Violação dos direitos de personalidade suscetível de ter sido cometida através da publicação de fotografias na Internet. Lugar onde ocorreu ou poderá ocorrer o facto danoso. Demandante: G. Demandado: Cornelius de Visser. Documento 62010CA0292. Data de Julgamento: 15/03/2012, Data de Publicação: 05/05/2012. Luxemburgo: EUR-Lex, 2012. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1490735881940&uri=CELEX:62010CA0292>. Acesso em: 28 mar. 2022.

UNITED STATES OF AMERICA. Federal Rules of Criminal Procedure. **Rule 41**: Search and Seizure. Washington: U.S. Government Printing Office, 2014. Disponível em: [https://www.law.cornell.edu/rules/frcrmp/rule\\_41](https://www.law.cornell.edu/rules/frcrmp/rule_41). Acesso em: 22 jan. 2022.

UPGUARD. Losing Face: Two More Cases of Third-Party Facebook App Data Exposure. **UpGuard**, Hobart, 03 Apr. 2019. Breaches. Disponível em: <https://www.upguard.com/breaches/facebook-user-data-leak>. Acesso em: 29 jan. 2022.

VAN DER SAR, Ernesto. TRON Cryptocurrency Founder Plans to Buy BitTorrent Inc. **TorrentFreak**, Manchester, 25 May 2018. BitTorrent. Disponível em: <https://torrentfreak.com/tron-founder-plans-to-buy-bittorrent-inc-180525/>. Acesso em: 22 abr. 2022.

VAN DER SAR, Ernesto. µTorrent is the Most Used BitTorrent Client By Far. **TorrentFreak**, Manchester, 05 Apr. 2020. News. Disponível em: <https://torrentfreak.com/utorrent-is-the-most-used-bittorrent-client-by-far-200405/>. Acesso em: 22 abr. 2022.

VASCONCELOS, Cláudio Lins de. As limitações, o fair use e a guinada utilitarista do direito autoral brasileiro. In: MARTINS, Guilherme Magalhães (coord.). **Direito privado e internet**. São Paulo: Atlas, 2014.

VAZ, Paulo; SÁ-CARVALHO, Carolina; POMBO, Mariana. Risco e sofrimento evitável: a imagem da polícia no noticiário de crime. **E-compós**, Brasília, DF, v. 4, p. 1-22, dez. 2005. DOI 10.30962/ec.46.

VEBLEN, Thorstein. **The Engineers and the Price System**. Kitchener: Batoche Books, 2001.

VENOSA, Sílvio de Salvo. **Direito Civil**: Responsabilidade Civil. 6. ed. São Paulo: Atlas, 2006.

VERBEEK, Peter-Paul. **What Things Do**: Philosophical Reflections on Technology, Agency and Design. University Park: The Pennsylvania State University Press, 2005.

VERIZON. 2019 Data Breach Investigations Report. **Verizon**, New York, 2019. Reports. Disponível em: <https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf>. Acesso em: 22 jan. 2022.

VIANA, Rui Geraldo Camargo; LIMA, Cintia Rosa Pereira de. Novas perspectivas sobre os direitos da personalidade. *In*: LIMA, Cíntia Rosa Pereira de; NUNES, Lydia Neves Bastos Telles. **Estudos Avançados de Direito Digital**. Rio de Janeiro: Elsevier, 2014.

VILAÇA, Murilo Mariano; DIAS, Maria Clara Marques. Transumanismo e o futuro (pós-)humano. **Physis**, Rio de Janeiro, v. 24, n. 2, p. 341-362, abr./jun. 2014. DOI 10.1590/S0103-73312014000200002.

VON SCHOMBERG, René. Introduction: Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. *In*: EUROPEAN COMMISSION. Directorate-General for Research and Innovation. **Towards responsible research and innovation in the information and communication technologies and security technologies fields**. Edition: René Von Schomberg. Luxembourg: Publications Office, 2011. DOI 10.2777/58723.

WANG, Stephen Jia. DMCA safe harbors for virtual private server providers hosting BitTorrent clients. **Duke Law Technology Review**, Durham, v. 12, issue 1, p. 163-181, 2014. Disponível em: <https://scholarship.law.duke.edu/dltr/vol12/iss1/9/>. Acesso em: 25 jan. 2022.

WIPO. World Intellectual Property Indicators. **WIPO**, Geneva, 2013. WIPO Economics & Statistics Series. Disponível em: [https://www.wipo.int/edocs/pubdocs/en/intproperty/941/wipo\\_pub\\_941\\_2012.pdf](https://www.wipo.int/edocs/pubdocs/en/intproperty/941/wipo_pub_941_2012.pdf). Acesso em: 22 jan. 2022.

WORLD TRADE ORGANIZATION. **Brazil – Measures Affecting Patent Protection (WT/DS199/4)**: Notification of Mutually Agreed Solution. Parties: United States and Brazil. Agreement date: 05/07/2001. Geneva: WTO, 2001. Disponível em: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q/IP/D/23A1.pdf&Open=True>. Acesso em: 28 maio 2022.

WÜEST, Candid. Underground black market: Thriving trade in stolen data, malware, and attack services. **Broadcom**, San José, 20 Nov. 2015. Symantec Enterprise. Disponível em: <https://community.broadcom.com/symantecenterprise/viewdocument/underground-black-market-thriving>. Acesso em: 12 fev. 2022.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019.